SafeNet LUNA® EFT

FIPS 140-2 LEVEL 3 SECURITY POLICY

DOCUMENT NUMBER:	CR-2786
AUTHOR(S):	Brian Franklin / Terry Fletcher / Chris Brych
DEPARTMENT:	Engineering
LOCATION OF ISSUE:	Ottawa
DATE ORIGINATED:	January 15, 2008
REVISION LEVEL:	15
REVISION DATE:	April 4, 2014
SUPERSESSION DATA:	14
SECURITY LEVEL:	Non-Proprietary

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Purpose

This document describes the security policy enforced by the SafeNet LUNA EFT.

This document applies to:

- Firmware Version MAL1.1 and Hardware Version GRK-15, Version Code 0100.

1.2. Scope

The security policy described in this document applies to the SafeNet LUNA EFT only and does not apply to any application firmware that may be loaded on the SafeNet LUNA EFT (hereafter referred to as “appliance” or “module”).

1.3. Intended Audience

The intended audience for this document is the SafeNet HSM Engineering and Product Management Team, external agencies for validation or endorsement of the SafeNet LUNA EFT module and selected industry partners and prospective customers.

1.4. Overview

The cryptographic module meets FIPS 140-2 Level 3 requirements as summarized below.

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

Table 1-1. FIPS 140-2 Security Requirements

2. SECURITY POLICY

2.1. Functional Overview

The appliance is a physically and logically secured appliance platform used as the host for the SafeNet LUNA EFT product line. The appliance's primary security service is to verify the digital signature of the LUNA EFT application firmware before allowing it to load. The appliance is a multi-chip standalone module that meets all FIPS 140-2 Level 3 requirements.

The appliance's loader firmware, which is installed during device manufacture, is included in the scope of the appliance validation. The loader firmware will only allow an application to be loaded if the application has been signed by a private key that corresponds to the public key embedded in the loader application. Loaded firmware must be separately validated in order for a product comprising the appliance plus application firmware to be considered FIPS validated.

The loader firmware is implemented as a 32-bit protected mode Intel executable and runs as the only application on a specially cut-down Fedora Core 3 (FC3) Operating System (O/S). The FC3 system launches the loader firmware and provides disk and memory management services and communication services to the loader firmware.

Figure 2-1. SafeNet LUNA EFT

2.2. FIPS-Approved Mode of Operation

The module implements the following FIPS-approved algorithms in the K5 HSM:

Approved Security Functions	***Certificate***
Symmetric Encryption/Decryption	
AES: ECB (e/d; Key Sizes = 128; 192; 256)	2629
Triple-DES (TECB(e/d ; KO 1,2); TCBC(e/d; KO 1,2))	1578
Random Number Generation	
ANSI X9.31 (3-Key Triple-DES)	1242

Table 2-1. FIPS Approved Algorithms in K5 HSM

The module implements the following FIPS Approved algorithms in MAL1.1 firmware:

Approved Security Functions	*Certificate*
Signature Verification	
RSA (Sig Ver PKCS#1 | 2048 | SHA-256)	1350
Secure Hash Standard	
SHA-256 (Byte Only)	2212

Table 2-2. Approved Algorithms in MAL Firmware

The module only contains FIPS Approved services and is always in FIPS Mode. If an application is loaded that has not been included as part of the FIPS certification, the module is not considered "FIPS Validated". The current mode is indicated by reviewing the console output.

It should be noted that the physical security of the appliance and the operation of the Random Number Generator are dependent on internal hardware features and not the firmware being loaded.

2.3. Cryptographic Module Ports and Interfaces

Front Panel Physical Interfaces

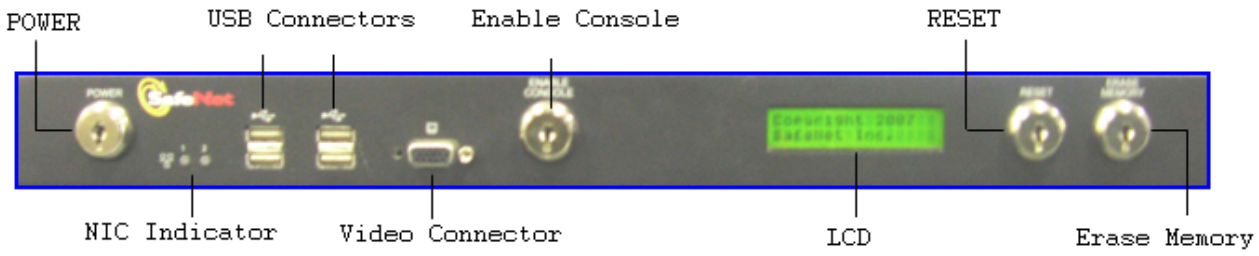


Figure 2-2. Front View – SafeNet LUNA EFT

The module has the following physical interfaces on the front panel:

- Four USB connectors
- One VGA output
- An LCD display on the front panel that displays system status information
- There are several physical key-activated switches on the front panel:
  a. A "POWER" on/off switch to control the device power.
  b. A "RESET" switch to command a device reset.
  c. A switch labelled "Enable Console" that enables the VGA output and USB connectors.
  d. A switch labelled "Erase Memory". The Erase Memory Key activates the tamper response circuit, which asserts the signal that erases the plaintext master key in the Real Time Clock (RTC) memory of the internal PCI card and also signals the ATX power supply to go to standby mode, removing main power from the motherboard and destroying DRAM contents. When the key switch is released (i.e., the tamper source is removed), the signal to the internal crypto card and the ATX is removed and the device is free to boot up again without any Critical Security Parameters (CSPs) being set.

Back Panel Physical Interfaces

The module has the following physical interfaces on the back panel:

- Main power socket (110 or 220 volt 50-60Hz)

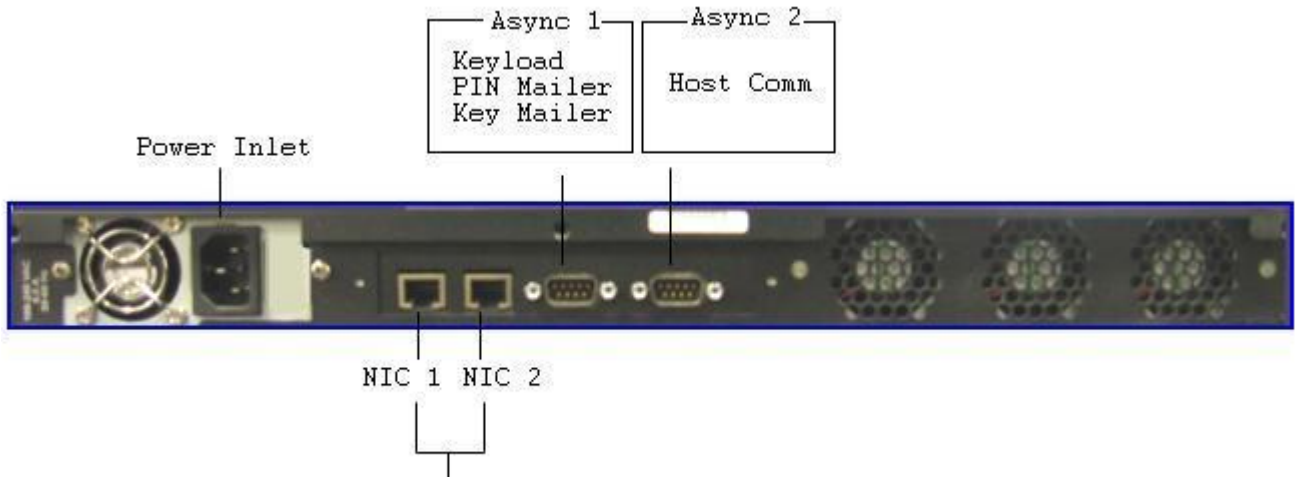


Figure 2-3. Back View - SafeNet LUNA EFT

- Two RS232 serial ports. These are referred to as the Keyload and Host Comm ports, but with the application loader firmware installed they have no security-related uses.
- Two RJ-45 10BaseT/100BaseTX/1000BaseTX Ethernet connections. One connection is used to receive application firmware updates and the other is reserved for future use.

Logical Interfaces

The module's physical interfaces are separated into logical interfaces, defined by FIPS 140-2, and described in Table 2-3. FIPS 140-2 Logical Interfaces:

FIPS 140-2 Logical Interfaces	Device Physical Interfaces
Data Input Interface	Ethernet port, USB ports
Data Output Interface	VGA port
Control Input Interface	Reset SW, Power SW, Erase Memory SW, Console Enable SW, USB ports
Status Output Interface	Ethernet port, LCD, VGA port
Power Interface	Main power socket

Table 2-3. FIPS 140-2 Logical Interfaces

3. ROLES AND SERVICES

3.1. Module Roles

The module supports two roles:

- Administrator – an authenticated operator performing administrative duties, the administrator is also authorised to load a signed application firmware package.
- Crypto Officer – an authenticated operator who performs some manufacturing duties

The Administrator role performs the verification of the signature on the application firmware to be loaded into the appliance.

Unauthenticated users may access non-cryptographic services provided by the module.

The services accessible from the module are described in section 3.2.

Authentication

The appliance implements identity-based operator authentication and assigns the Crypto Officer or Administrator role based on the type of authentication used.

The identity associated with the module's Crypto Officer is the manufacturer. The manufacturer first initializes the appliance by installing the loader firmware and the public key into the module.

The authentication data required of the manufacturer in the Crypto Officer role is password-based.

In the Administrator role, the manufacturer or authorized agent uses the Console interface to load the signed application, which in turn invokes the signature verification service. The Administrator is authenticated by a password entered through the Console interface. The authentication verification data is a copy of the password entered previously by the Administrator and stored inside the module protected with Triple-DES CBC encryption.

Strength of Authentication Mechanisms

Since the size of the search space required to recover a private key for 2048-bit RSA is 2^{112}, the probability that a random attempt to use the authentication mechanism will succeed or that a false acceptance will occur is significantly less than one in 1,000,000. There is a practical maximum of 15 verification attempts possible in a minute (selecting and verifying signed binaries) versus a total space of 2^{112} or (reducing by 10^{20}) 51,922,968,585,348 possible signed binaries, which becomes a 1/3,461,531,239,023 chance of succeeding in a minute. Since authentication depends on signature verification as a part of the application loading process, the probability that multiple attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is significantly less than one in 100,000.

The Administrator and Crypto Officer passwords are alpha-numeric strings from 8 to 15 characters long. Both uppercase and lowercase alphabetical characters are allowed as well as punctuation marks and the space character. There are at least 88 different characters possible for each character in the password. With a minimum of 8 characters, this means that there are at least 88^8 or 3.5×10^{15} possible passwords[1]. The probability that a random attempt to use the authentication mechanism will succeed or that a false acceptance will occur is significantly less than one in 1,000,000. There is a practical maximum of 30 authentication attempts possible in a minute versus a total space of possible combinations of 88^8 or 3,596,345,248,055,296 different signatures. This becomes a 30/3,596,345,248,055,296 or 1/119,878,174,935,177 chance of succeeding in a minute. Since the authentication process must be performed by an operator via the console interface (i.e., cannot be automated) the probability that multiple attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is therefore significantly less than one in 100,000.

[1] The actual space is 3,596,345,248,055,296 possible passwords.

3.2. Module Services

The only two cryptographic (or supporting) services provided by the module are operator authentication (Administrator) and the verification of the digital signature on application firmware to be loaded into the device. The Administrator automatically invokes the signature verification service with an attempt to load an application.

The Administrator also has these management services available:

- Change the Administrator password
- Generate module master key
- Selectively enable and disable TCP/IP Host port functions
- Set TCP/IP network parameters
- Run self-tests and view device status statistics
- View the upgrade public key fingerprint
- Reboot the device (resets the module without losing CSPs)
- Verify and install application firmware package obtained from a mass storage device on an USB port, or previously loaded by host port function
- Encrypt / Decrypt with module master key

The Crypto Officer has these management services available:

- View the status on the Console
- View device status statistics
- Initial installation and configuration of firmware at manufacturing time
- Change the Crypto Officer password
- Encrypt / Decrypt with module master key

The following non-cryptographic services are also available to unauthenticated operators in physical proximity to the device:

- Reboot unit (resets the module without losing CSPs)
- Erase memory (using front panel keyed switch)
- Disable Console (force Administrator to log off using front panel keyed switch)
- View the status on the LCD display

The following non-cryptographic services are also available to unauthenticated operators accessing the TCP/IP host port:

- Low level network services ICMP (Ping) ARP
- Status Query functions (HSM_STATUS, HSM_ERRORLOG_STATUS, HSM_GET_ERRORLOG, GET_VERSION, HSM_SOFTWARE_STATUS)
- Self-test functions (TEST_PORT, TEST_CRYPTO, GEN_RNG_RSA)
- The LOAD_HSM_SOFTWARE function provides one of several methods to present the application firmware package to the Administrator. This function does not cause the firmware to be verified or installed.

4. SELF-TESTS

The LUNA EFT performs the following power-up self-tests automatically on power-up of the module:

- Firmware integrity test using a SHA-256 EDC.
- AES e/d KAT;
- Triple-DES e/d KAT;
- RSA 2048 verify KAT;
- SHA-256 KAT; and
- ANSI X9.31 KAT.

If the EDC test or any one of the KAT tests fails, the module returns the status message "FIPS_SELFTESTFAILCODE" and the code ID. The error is logged and the module goes into the error state.

The module supports conditional RNG and firmware load tests. Conditional RNG self-tests are applied to approved and non-approved RNG output to verify the module is not generating the same output. Firmware loaded onto the module is verified for authenticity by an RSA 2048 bit public key certificate.

5. ACCESS CONTROL POLICY

The Crypto Officer is authorized to install the application loader firmware, which includes the SafeNet public key, into the module at the manufacturing facility. The application loader firmware will prevent itself from being overwritten by anything other than a validly signed application once it is installed. This is to prevent a potentially malicious version of the firmware, with a forged certificate representing a rogue signing key, from being installed before the application is loaded.

The Administrator is authorized to perform signature verification as part of the application-loading service provided by the module.

An operator may also perform other services provided by the module (see Section 3.2).

6. CRITICAL SECURITY PARAMETERS

The only cryptographic key directly employed by the module is the public key component of the SafeNet application firmware verification key pair. This is stored on the internal hard disk in plaintext form and is protected by the physical and logical security mechanisms associated with the appliance. The public key remains with the module throughout its operational life. Although disclosure of the public key does not constitute a security risk, replacement of the public key would enable an attacker to sign malicious applications using a rogue private key and thereby potentially cause damage to a customer's application system.

There is one password stored on the device that is used to authenticate the Administrator. The password is stored in an encrypted form (Triple-DES CBC) on the appliance hard disk. The encrypting key is held in tamper responding memory within the internal crypto card.

Private keys are not stored or used by the module.

The RNG Seed Value and RNG Seed Key are automatically zeroized when the module is powered off.

CSP	CSP Type	Generation	Input/Output	Storage	Destruction Mechanism	Use
Public Key Certificate	2048 bit RSA	N/A	input	Plaintext in Flash	None	To verify the signature attached to a new firmware image.
Password	password	manual	input	Encrypted with Module Master Key	Tamper or Erase Memory Key on appliance	To permit login by Administrator or Crypto Officer
RNG Seed Value	Seed data (64 bits)	H/W RNG	Not input/output	Not permanently stored, working memory only	Tamper or Erase Memory Key on appliance	Used as part of the RNG process.
RNG Seed Key	3-Key Triple-DES	H/W RNG	Not input/output	Not permanently stored, working memory only	Tamper or Erase Memory Key on appliance	Used as part of the RNG process.
Module Master Key	AES-256, Triple-DES	ANSI X9.31 RNG	Not input/output	Tamper responsive memory in NVRAM of RTC	Tamper or Erase Memory Key on appliance	Used to encrypt contents of secure memory

Table 6-1. List of Keys Stored in Module

6.1. Access Control

The following table shows each key or CSP along with the type of access for each role.

R - The item is **read** or referenced.

W - The item is **written** or updated.

X - The item is **executed**. (The item is used as part of a cryptographic function.)

D - The item is **deleted**.

Service / Role	Key or CSP	Access Control
Verify signed image / Administrator / Crypto Officer	RSA Public Key	R / R
Change password / Administrator / Crypto Officer	User Password	W / W
Run self-test / Administrator	RNG Seed Value RNG Key Value	R,X R,X
View Upgrade Public Key Certificate / Administrator	RSA Public Key	R
Erase memory / Administrator / Crypto Officer	RNG Seed Value RNG Key Value Module Master Key	D / D D / D D / D
Initialize appliance / Administrator	Module Master Key	W
Encrypt/Decrypt – Administrator / Crypto Officer	Module Master Key	X,D / X,D
Generate Module Master Key / Administrator	Module Master Key	W,X,D

Table 6-2. Access Controls for CSPs

7. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Operational Environment requirements are not applicable, because the appliance's cryptographic module does not contain a modifiable operational environment. The module only supports the loading of application firmware that is properly signed by the SafeNet application signing authority. In order for the appliance to continue in a FIPS-approved mode of operation after loading an application, the application itself must have been separately validated.

8. PHYSICAL SECURITY

The appliance is a tamper-resistant multiple-chip standalone cryptographic module consisting of production grade components intended to meet FIPS 140-2 Level 3. It does not support a maintenance role and therefore security concerns arising from such a role are not relevant.

The appliance is contained in a hard metal enclosure with double louvers and baffles to prevent probing. The enclosure is sealed using break-away screws and tamper-evident seals that are applied at manufacturing to prevent easy removal of the enclosure's lid and to provide tamper evidence in the event the lid is forced off in some way.

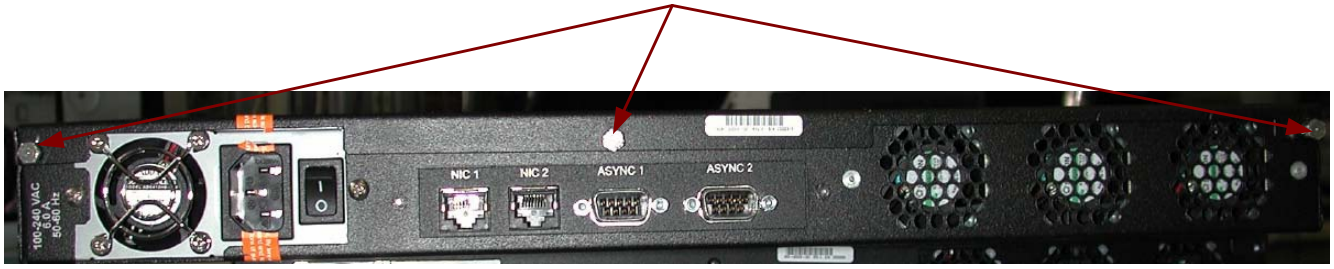
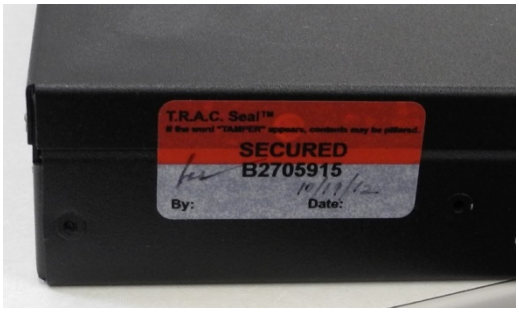


Figure 8-1. Break-away crews at rear of appliance



Left (No. 1)

Right (No. 2)

Figure 8-2. Two Serialized Tamper-Evident Seals (at rear corner of each side of appliance)

The module should be periodically inspected for evidence of tamper (note that only the corner red and white labels shown in Figure 8-2 provide tamper evidence). If the module's enclosure shows signs of tamper, the module shall be zeroized and the module must be re-initialized.

The appliance also contains tamper switches that are triggered in the event the lid is removed. If any of the switches are triggered, the module will immediately clear any sensitive application data, power down and prevent access to the loader firmware.

9. GLOSSARY OF TERMS, ACRONYMS AND ABBREVIATIONS

Terms	Definitions
10BaseT/100BaseTX	Ethernet over twisted pair (10 Mbit/s and 100Mbit/s)
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ATX	Advanced Technology Extended
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DRAM	Dynamic Random Access Memory
EDC	Error Detection Code
FC3	Fedora Core 3
FIPS	Federal Information Processing Standard
ICMP	Internet Control Message Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
NIC	Network Interface Controller
O/S	Operating System
PCI	Peripheral Component Interconnect
RJ-45	8 position 8 contact (8P8C) modular communications connection
RNG	Random Number Generator
RSA	Rivest, Shamir, Adelman
SHA	Secure Hashing Algorithm
Triple-DES	Triple-DES
TCP/IP	Transport Control Protocol / Internet Protocol
USB	Universal Serial Bus
VGA	Video Graphics Array