SafeNet Ethernet Encryptor, Branch Office

for 10 Megabit Networks

FIPS 140-2 – Level 3 Validation
Non-Proprietary Security Policy

Hardware Part Number
943-50200-004

with 1.0.6.4 firmware

Security Policy Revision B
June 2010

---

 www.safenet-inc.com 009886-001 Revision B

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

1.1 Overview

This document is the Security Policy for the SafeNet Ethernet Encryptor, Branch Office (SEE BO) manufactured by SafeNet, Inc. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 3. It describes how the encryptor functions in order to meet the FIPS requirements, and the actions that operators must take to maintain the security of the encryptor.

This Security Policy describes the features and design of the SEE BO using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CSEC Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard, and information on the CMVP, can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html. More information describing the SafeNet Ethernet Encryptor, Branch Office can be found at http://safenet-inc.com.

This Security Policy defines the cryptographic module operating at 10MB.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “SafeNet - Proprietary” and is releasable only under appropriate non-disclosure agreements.

1.2 References

Document No.	Author	Title
FIPS PUB 140-2	NIST	FIPS PUB 140-2: Security Requirements for Cryptographic Modules
FIPS PUB 140-2 Annex A	NIST	FIPS 140-2 Annex A: Approved Security Functions
FIPS PUB 140-2 Annex B	NIST	FIPS 140-2 Annex B: Approved Protection Profiles
FIPS PUB 140-2 Annex C	NIST	FIPS 140-2 Annex C: Approved Random Number Generators
FIPS PUB 140-2 Annex D	NIST	FIPS 140-2 Annex D: Approved Key Establishment Techniques
DTR for FIPS PUB 140-2	NIST	Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
FIPS PUB 46-3	NIST	Data Encryption Standard (DES)
FIPS PUB 81	NIST	DES Modes of Operation
FIPS PUB 186-2	NIST	Digital Signature Standard (DSS)
FIPS PUB 180-1	NIST	Secure Hash Standard (SHS)

All of the above references are available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.3 Terminology

In this document, the SEE BO is also referred to as “the module” or “the encryptor”.

1.4 FIPS Requirements

The encryptor meets the overall requirements applicable for FIPS 140-2 Level 3 security as shown in Table 1.4-1.

Table 1.4-1 – Cryptographic Module Security Requirements

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	3

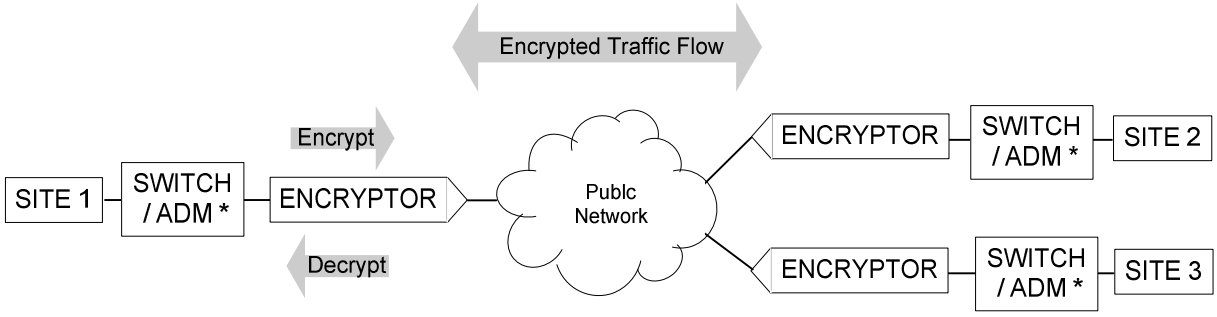
2 SafeNet Ethernet Encryptor Branch Office

2.1 Functional Overview

The SafeNet Ethernet Encryptor, Branch Office provides data privacy and access control for connections between vulnerable public and private networks. It employs a FIPS-approved AES algorithm and can be deployed in 10/100 Megabit Ethernet networks. The encryptor can be centrally controlled or managed across multiple remote stations using SafeNet's Security Management Center (SMC), a SNMPv3-based security management system.

The role of the encryptor is illustrated in Figure 2.1-1. The encryptor is installed between private network equipment and a public network. An encryptor communicates with other encryptors in the network, establishing secured connections between itself and the other modules. The encryptors selectively encrypt, zeroize, or pass in the clear, data flowing from the switch to the network. Conversely the encryptors selectively decrypt, reject, or pass information flowing from the network to the switch.

Figure 2.1-1 – Encryptor Operation



Secured connections are established between the cryptographic module and similar units using the RSA key exchange process (as specified in the ATM Forum Security Specification version 1.1). This results in a separate secure session and does not require any secret session keys to ever be displayed or manually transported and installed.

Figure 2.1-2- Encryptor Usage in Path Encryption Mode

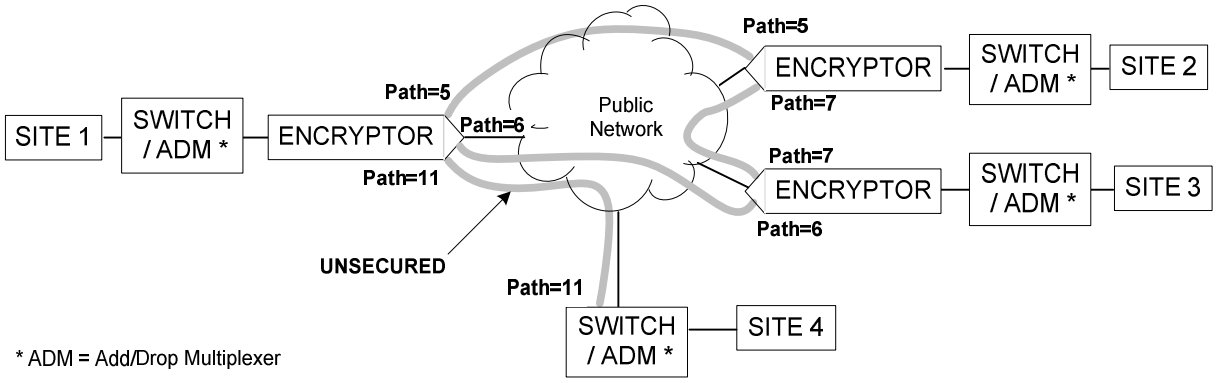


Figure 2.1-2 shows an example of three secured paths and one unsecured path between sites.

Figure 2.1-3– Encryptor Usage in Line Encryption Mode

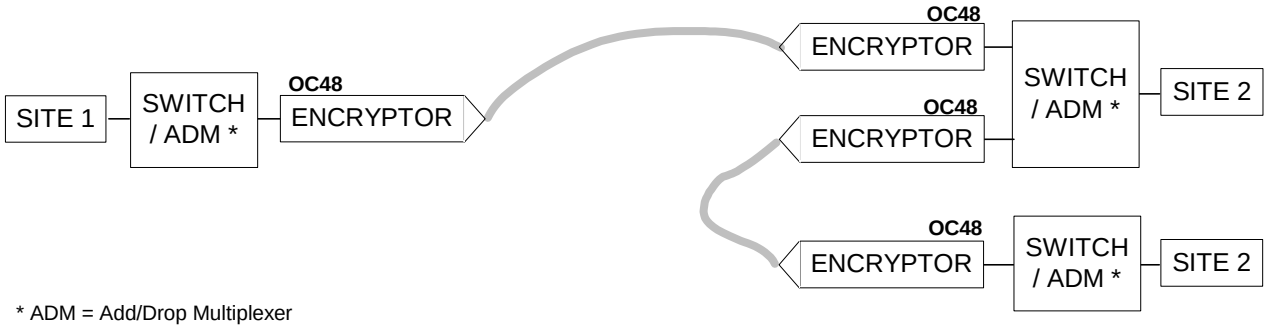


Figure 2.1-3 shows an example using encryptors in line encryption mode.

2.2 Module Description

The SEE BO is a multiple-chip standalone cryptographic module consisting of production-grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 3. The module outer casing defines the cryptographic boundary. The encryptor is enclosed by a metal case to protect it from tampering. Any attempt to remove the cover will automatically erase all sensitive information stored internally in the encryptor.

Table 2.2-1 – Supported Model

SafeNet Ethernet Encryptor Branch Office (SEE BO)	943-50200-004

Module management is provided in-band or out-of-band. In-band management uses management channels on the module's interface ports. Out-of-band management is provided using the dedicated Ethernet port or a console port.

2.2.1 Enclosure Indicators Connectors and Controls

Figure 2.2-1 shows the front view. The front panel provides status LEDs.

Figure 2.2-1 – Front View of Branch Office Encryptor

Figure 2.2-2 shows the rear view. The rear panel provides a console port, the local and network port interfaces, a management port, and the power connector.

Figure 2.2-2 – Rear View of Branch Office Encryptor

The encryptor has three network interfaces located in the back of the module: the Local Port interface connects to a physically secure private network, the Network Port interface connects to an unsecure public network, and the LAN/Management interface provides for remote management. The rear panel network interfaces contain network activity LEDs. Two tamper evident seals indicate the physical security of the module is intact and the module has not been tampered.

2.2.1.1 Front Panel Physical Interface

- The **LEDs** indicate the state of the system including alarms.

2.2.1.2 Rear Panel Physical Interfaces

- The DB9 **RS-232** serial console port connects to a local terminal and provides a command line interface for initialization prior to authentication and operation in the approved mode. This port also allows administrative access and monitoring of operations. Access is protected by user names and passwords.
- The **Network Port** connects to the public network via the network RJ45 connector. Access is protected by RSA certificates. The Local Port and Network Port are of the same interface type.
- The **Local Port** connects to the private network via the local RJ45 connector. Access is protected by RSA certificates. The Local Port and Network Port are of the same interface type.
- The **LAN / MGMT Port** RJ45 connector allows remote management from the SMC application. Access is protected by SNMPv3 security mechanisms for authentication and data encryption.
- The **LEDs** indicate network traffic on each port.
- The **power connector** is used for power input to the module.

The logical interfaces consist of Data Input, Data Output, Control Input, and Status Output as follows:

Table 2.2-2 – Cryptographic Module Logical Interfaces

Logical Interface	Description
Data Input Data Output	**Local Port:** • Connects to the private network via the RJ45 Ethernet connector, sending and receiving plaintext user data. **Network Port:** • Connects to the public network via the RJ45 Ethernet connector, sending and receiving ciphertext and plaintext user data to and from a far end module. • Sends authentication data and RSA key exchange components to a far end module. • Receives authentication data, RSA key exchange components from a far end module. • The module can be set to bypass, to send and receive plaintext for the selected connection.
Control Input	Control Input is provided by the serial port, the LAN / Management Port (out-of-band control), and the Local and Network ports (in-band control) as follows: • The DB9 RS-232 serial console port may be used for initialization prior to authentication and operation in the approved mode. This port receives control input (protected via a username and password) from a locally connected terminal. • The LAN / Management Ethernet port receives out-of-band control input from the SMC application. • The Local and Network ports may receive in-band control input, protected via the SNMPv3 security mechanisms, from the SMC application.
Status output	Status output is provided by the front and rear panel LEDs, the DB9 RS-232 port, the LAN / Management Port (out-of-band status), and the Local and Network ports (in-band status) as follows: • Front and rear panel LEDs indicate error states, state of the local and network interfaces, alarm, temperature, and battery state. • The DB9 RS-232 serial console port may be used for monitoring some operations. This port sends status output (protected via a username and password) to a locally connected terminal. • The LAN / Management Ethernet port sends out-of-band status output information to an SMC application. • The Local and Network ports may send in-band status output information, protected via the SNMPv3 security mechanisms, to the SMC application.

Table 2.2-3 maps FIPS 140-2 logical interfaces to the cryptographic module's logical interfaces and physical ports.

Table 2.2-3 – Mapping of Logical Interfaces to Physical Ports

FIPS 140-2 Logical Interface	Logical Interface	Physical Port
Data Input	1) Public network interface 2) Private network interface	1) Rear panel Network Port 2) Rear panel Local Port
Data Output	1) Public network interface 2) Private network interface	1) Rear panel Network Port 2) Rear panel Local Port
Control Input	1) SNMPv3 interface 2) Local console 3) Public network interface 4) Private network interface	1) Rear panel LAN / Management Port 2) Rear panel DB9 RS232 serial console port 3) Rear panel Network Port 4) Rear panel Local Port
Status Output	1) SNMPv3 interface 2) Local console 3) Front Panel Display	1) Rear panel Local / Network Ports 2) Rear panel DB9 RS232 serial console port 3) Front and rear panel LED displays
Power	Power Switch	Rear panel power connector

The encryptor may permit logically distinct categories of information to share the network port. The Configuration Action Table may be configured to allow in-band management traffic such that control/status data (key exchange or management commands) and user data enter, and exit, the module over the network port.

2.3 Security Functions

The module provides symmetric key encryption (AES) for user data transferred through the module. AES is also used to secure the remote management interface to the module. Asymmetric keys and SHA hashing are used to authenticate remote modules, and asymmetric keys are used to wrap symmetric keys for symmetric key exchange with other modules. Asymmetric keys and SHA hashing are used to authenticate management access, and Diffie-Hellman key agreement is used to establish symmetric keys for securing management interactions.

To ensure maximum security, unique encryption keys are automatically generated for a connection only after the encryptor has positively identified and authenticated the remote module.

The encryptor implements the following approved algorithms:

Table 2.3-1 – Approved Module Algorithms

Approved Algorithm	CAVP Certificate
AES (FIPS PUB 197) ECB(e only; 256); CTR(int only; 256); CBC(e/d; 128); CFB128(e/d; 128, 256)	1243
Triple-DES (FIPS PUB 46-3) TCFB8(e/d; KO 1)	890
Hashing SHA-1 (byte-oriented hashing) HMAC-SHA-1	1142 740

Approved Algorithm	CAVP Certificate
Random Number Generation	
ANSI X9.31 [AES-256]	690
Digital Signatures	
Key Gen ANSI X9.31 (MOD: 1024 | Pubkey Values: 65537)	596
Sig Gen PKCS#1/ Sig Ver PKCS#1 | 1024 | SHA-1	596

Note 1: A software-based noise source library is used as a non-Approved RNG to generate seed material (consisting of random sequences of ones and zeroes) for the FIPS-approved RNG.

In addition to the approved algorithms, the module may also employ two non-approved algorithms when operating in the non-FIPS mode. The non-approved algorithms employed in the module are:

- Camellia (CFB with key length 256)
- SEED (CFB with key length 128)

The encryptor implements the following security functions:

Table 2.3-2 – Module Security Functions

Security Function
Symmetric Key Encryption
AES
Triple-DES
Symmetric Key Establishment (See Note below this table)
RSA key establishment (per ATM Forum Security Spec 1.1)
Diffie-Hellman key agreement Public Key Length: 1024 bits Private Key Length: 1023 bits
Authentication
RSA asymmetric key 1024-bit (per ANSI X9.31)
HMAC SHA-1
Key Generation
Triple-DES/AES Keys – PRNG (per ANSI X9.31)
RSA keys – ANSI X9.31

Note – Key establishment methodology provides 80-bits of encryption strength.

2.4 Modes of Operation

The module is shipped by the manufacturer with the FIPS approved mode of operation enabled. FIPS-Mode operation may be turned off as needed. When FIPS-Mode operation is turned off, the SNMPv3 Privacy option may be disabled and the non-approved algorithms may be used. To turn FIPS-Mode operation back on, SNMPv3 Privacy must first be enabled. The FIPS mode status may be queried from the management application or the console interface. Operators may run the power-on self-tests on-demand by power-cycling the module. Refer to the User's Guide for more details concerning FIPS operation and SNMPv3 privacy.

User data received from the local (private) network is encrypted before being transmitted out to the public network. Similarly, user data received from the public network is decrypted before being transmitted to the local network.

Each encryptor must have a unique Network Certificate (NC) issued under a common Security Management Center (SMC). During key exchange, communicating modules mutually authenticate one another by exchanging NCs in digitally-signed messages. The module cannot build a secure connection with a remote module that does not have a valid NC. Moreover, the module cannot establish any connections unless it has been issued a valid NC. This mode of operation requires a common SMC to issue NCs to all modules that will communicate securely.

When a secure connection is first created, the pair of encryptors exchange an encryption master key and session key. The master key is used for all subsequent session key exchanges. When operating in this state, the two ends of the connection are in cryptographic synchronization using the defined AES algorithm. Crypto officers can force a new master key by manually restarting a connection. An organization's security policy dictates the frequency of forcing a new master key. Within a secure connection, the module encrypts all data received from the Local Port (the private network) and decrypts all data received from the Network Port (the public network).

For each connection, the Connection Action Table can be set to encrypt, block, or pass data. The module supports configured encryption, blocking, or passing of user data as plaintext on a per-connection basis.

2.4.1 FIPS Approved Mode

The module ships with FIPS Mode enabled. In this mode the privacy of the SNMPv3 based management interface is ensured with AES encryption, and all the algorithms accessible to the module are approved algorithms as noted above. Non-approved algorithms cannot be specified for use and the SNMPv3 privacy feature cannot be disabled.

FIPS Mode operation can be confirmed by logging into the console interface and using the fips command. It can also be confirmed by reviewing the device configuration from SMC. The module front panel SEC LED provides details about the operational configuration of the device, as detailed in the User's Guide, but does not specifically indicate the FIPS Mode status of the module.

When changing from FIPS Mode to non-FIPS Mode operation, a module erase and reboot is forced. This effectively zeroizes all keys and CSPs prior to the transition.

2.4.2 Non-FIPS Approved Mode

Non-FIPS Mode operations follow the same general flow as FIPS Mode. The module must be certified, connections must be configured and the encryptors must still authenticate to each other with NCs. When the module is set, by a Crypto Officer, to operate in non-FIPS approved mode:

- SNMPv3 commands need not be encrypted; the SNMPv3 privacy feature may be disabled or enabled as needed
- The following algorithms may be used in conjunction with the connection between encryptors:
    - Camellia (CFB with key length 256)
    - SEED (CFB with key length 128)

    Note: No FIPS claims are made for the Camellia and SEED algorithms.

When changing from non-FIPS Mode to FIPS Mode operation, SNMPv3 privacy must be specifically enabled. The non-approved algorithms are disabled within the module automatically, but FIPS mode cannot be set if SNMPv3 privacy is disabled. Prior to the completion of the change, a module erase and reboot is forced. This effectively zeroizes all keys and CSPs prior to the transition.

2.5 Identification and Authentication

The module supports two Crypto Officer roles and a single Network User role. Services for the Crypto Officer roles (full access and read only) are accessible directly via the console or remotely via the SMC application. The Network User role services are only accessible indirectly based on the configured connections with other cryptographic modules. Roles cannot be changed while authenticated to the module.

Access to the authorized roles is restricted as follows in Table 2.5-1:

Table 2.5-1 – Roles with Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer (Full Access)	Identity-based	Crypto Officers using the CLI present unique user names and passwords to log in to the CLI. Crypto Officers using SMC present unique identities (embedded in the SNMPv3 command protocol).
Crypto Officer (Read Only)	Identity-based	Crypto Officers using the CLI present unique user names and passwords to log in to the CLI. Crypto Officers using SMC present unique identities (embedded in the SNMPv3 command protocol).
Network User	Identity-based	Network Users (remote encryptors) must present a certificate issued by the SMC.

Multiple concurrent Crypto Officers and Network Users are allowed. For example, a Network User may be sending data to the data input port while a Crypto Officer is connected via the console or sending an SNMPv3 command to the module. The architecture of the system allows for simultaneous interactions with many far end systems, or Network Users. Access control rules, system timing, and internal controls maintain separation of multiple concurrent Crypto Officers and Network Users.

The module employs identity-based authentication of operators and users. Up to 30 unique names and passwords can be defined for operators of the module.

- Crypto Officers using the console enter their name and password to authenticate directly with the module.
- Crypto Officers using SMC to issue SNMPv3 commands to the Encryptor, use SNMPv3-based authentication to establish a secure connection / tunnel to the module. Within the secure tunnel, SNMPv3 commands are individually authenticated to ensure Data Origin Authentication, and Data Integrity for all commands sent from SMC. Data Origin Authentication, based on the above names and passwords, ensures the authenticity of the identity of the user claiming to have sent the command.
- Users (Network Users) using the module cryptographic algorithms and security functions over the Data Input and Output ports authenticate using certificates that have been generated and signed by the SMC. These Network Users exchange master and session keys using RSA public key certificates that have been generated and signed by a common SMC.

Physical Maintenance is performed at the factory, as there are no services that require the cover to be removed in the field. The module should be zeroized, using the erase command, by a Crypto Officer before the module is returned to the factory.

The strength of the authentication, per the above roles, is as follows:

Table 2.5-2 – Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Authentication Password	Crypto Officers accessing the module using the CLI (via the console port) must authenticate using a password that is at least 8 characters and at most 30 characters. The characters used in the password must be from the ASCII character set of alphanumeric and special (shift-number) characters. - This yields a minimum of 62^8 (over 218 trillion) possible combinations (8 characters, 62 possibilities per character); thus, the possibility of correctly guessing a password is less than 1 in 1,000,000. - After three failed authentication attempts via the CLI, console port access is locked for 3 minutes; thus, the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. Note: the module suppresses feedback of authentication data being entered into the CLI by returning blank characters.
Authentication from SMC	Authentication with SMC is accomplished via SNMPv3 and the Authentication Password described above. - Based on the noted characteristics of the password, the possibility of correctly guessing the authentication data is less than 1 in 1,000,000. - The multi-step handshaking process for establishing a connection and then issuing an authenticated command sets the possibility of randomly guessing the password in 60 seconds at less than 1 in 100,000.
Network User Certificates	Network Users must authenticate using a 1024-bit RSA authentication certificate based on a key of similar size. - The possibility of deriving a private RSA key is less than 1 in 1,000,000 and the possibility of randomly guessing the key in 60 seconds is less than 1 in 100,000. - The multi-step handshaking process for establishing a connection sets the possibility of randomly guessing the authentication data in 60 seconds at less than 1 in 100,000.

2.5.1 Cryptographic Keys and CSPs

Table 2.5-3 identifies the Cryptographic Keys and Critical Security Parameters (CSPs) employed within the module.

Table 2.5-3 - Cryptographic Keys and CSPs

Data Item	Description
System Master Key	On initialization, the module generates a 168-bit symmetric key that is stored in the clear in battery-backed RAM. • This key encrypts (using 3-key Triple-DES CFB8) the module's public and private RSA keys and the user table stored in the configuration flash memory. • On tamper, the module zeroizes the System Master Key (SMK), rendering the encrypted data in the flash memory undecipherable.
RSA Private Key	The secret component of the module's RSA Key pair. • This 1024-bit key is generated when the module receives a load certificate command from the SMC, and is used to authenticate sessions with other encryptors and to unwrap master session keys and session keys received from far-end encryptors. • This key is stored encrypted in flash memory. • On tamper, the SMK is zeroized, rendering the encrypted private key undecipherable.
RSA Public Key	The public component of the module's RSA Key pair is stored encrypted in flash memory. • This key resides in the Network Certificate that in turn is stored in the clear in the module's non-volatile RAM. • This key is used for authenticating connections with other encryptors.
Authentication Password	Up to 30 passwords (and associated usernames) may be stored to allow access by up to 30 unique operators in the role of Crypto Officer (full access) or Crypto Officer (read only). • The CLI uses the authentication password to authenticate Crypto Officers accessing the system via the console port. • SNMPv3 concatenates and hashes (with SHA-1) the authentication password (8-30 characters) and the SNMPv3 unique engine ID to create an HMAC key used for Data Origin Authentication, and Data Integrity of each command. • Passwords and usernames are hashed and stored in the encrypted user table in flash memory. • On tamper, the System Master Key is zeroized, rendering the encrypted passwords undecipherable.

Data Item	Description
Management Privacy Key	The Management Privacy Key (MPK) is the parameter that is used to secure data on the remote management channel. This parameter is essentially a key that is derived from a DH key exchange between the module and the remote management station. • The MPK persists for the life of the management session and is used to AES encrypt management traffic that may be exchanged between the module and the remote management station. • The MPK is maintained in volatile memory and may be updated periodically during the session. • The MPK is destroyed at the end of a session.
Master Session Key	For each session, the module generates a symmetric Master Session Key (MSK) and Session Keys using the ANSI X9.31 PRNG. • The MSK is used with RSA key exchange to transfer these keys to a far-end encryptor for data encryption and decryption purposes. • The MSK persists for the life of the session and is used to AES-encrypt session keys that may be changed periodically during the session. • All session keys are destroyed at the end of its session.
Session Keys	For each session the module generates two Session Keys (SKs) for each data flow path in a secure connection (one for the Initiator-Responder path and another for the Responder-Initiator path). • These keys are used to AES-encrypt user data transferred between encryptors. • SKs may be changed periodically during the session based on time or based on the amount of data transferred. • All SKs are destroyed at the end of a session.
Network Certificate	The Network Certificate (NC) is the X.509v3 certificate associated with the module in an operational environment. • The NC is produced and signed by the managing SMC system, then stored in the clear in the module's non-volatile system RAM and used for authenticating connections with other encryptors. • Other encryptors use the public key embedded in the NC to wrap initial SKs used to encrypt a session with AES. • The NC is deleted from memory only on an Erase command from a module operator or a tamper condition.
PRNG Seed Key	A new ANSI X9.31 RNG Seed Key is generated from a block of 160 bits output by the random noise source software library. • The Seed Key is not stored and is never output from the module. It exists temporarily in volatile memory and is zeroized by power cycling the module.
PRNG Seed Value	A new ANSI X9.31 RNG Seed Value is generated from a block of 160 bits output by the random noise source software library. • The Seed Value is not stored and is never output from the module. It exists temporarily in volatile memory and is zeroized by power cycling the module.

Note: While the above table lists the certificates maintained within the module, the certificates contain only public information.

The module prevents data output during initialization and self test.

- No data is output from the module until the self tests complete successfully and the NC has been properly loaded into the module.
- No data is output during and after zeroization of cryptographic keys and CSPs as this occurs when a tamper condition exists.
- The encryptor's internal modules and timing controls work together to isolate user data input and output processes from CSP and key management functions.

2.5.2 Roles and Services

The encryptor supports services that are available to Crypto Officers and Users. All of the services are described in detail in the module's User's Guide and in the SMC User's Guide.

The Crypto Officer (full access) role provides cryptographic initialization and management functions. Crypto Officer functions are available using SMC and via the console CLI.

The Crypto Officer (read only) role is restricted to read-only access to module configuration data.

The Network User Role can negotiate encryption/decryption keys and use encryption/decryption services. (The Network User Role is available only to, or in conjunction with, other authenticated modules.)

Table 2.5-4 shows the services available to the various roles. All services except Run Self Test (Power Cycle the Module), AES or Triple-DES encryption, SHA-1 hashing for password verification, and physical tamper, require a console operator to be authenticated by entering a username and password, or an SMC operator to use RSA public key authentication and SNMPv3 user authentication.

Table 2.5-4 - Roles and Services

Service	No Role	Crypto Officer (Full Access)	Crypto Officer (Read Only)	Network User
Load Initial Network Certificate		●		
Load Subsequent Network Certificate		●		
Set Real Time Clock		●		
Edit Connection Action Table		●		
View Connection Action Table		●	●	
Create user accounts		●		
Modify user accounts		●		
Delete user accounts		●		
Show Software Version		●	●	
View User Accounts		●	●	
Clear Audit Trail		●		
View Audit Trail		●	●	
Clear Event Log		●		

Service	No Role	Crypto Officer (Full Access)	Crypto Officer (Read Only)	Network User
View Event Log		●	●	
View FIPS Mode Status		●	●	
Change SNMPv3 Privacy Mode		●[4]		
Run Self Test (Power Cycle the Module)	●			
Run Self Test (Reboot Command)		●		
Generate AES session keys		●[1]		●
Generate Initialization Vector		●[1]		●
Agree on management privacy key		●[5]	●[5]	
RSA signature generation		●[1]		●
RSA signature verification		●[1]		●
AES encryption		●[2],[5]	●[5]	●
AES decryption		●[2],[5]	●[5]	●
Triple-DES encryption and decryption (for the master secret)		●		
SHA Hashing for password verification	●			
Generate DH keys				●
DH Key Agreement		●[1]		●
Software load test		●		
Erase unit (Console Command)		●[3]		
Tamper	●			
Set FIPS Mode		●		

[1] Restarting a connection causes new session keys to be generated.
[2] Plaintext data entering the Local Port is encrypted, and ciphertext data entering the Network Port is decrypted, if the connection is set to encrypt data.
[3] Erasing the content of the module zeroizes the module.
[4] The SNMPv3 Privacy Mode may only be changed when FIPS Mode is turned off. Privacy must be enabled before FIPS Mode can be turned on.
[5] When Privacy is enabled, all remote management connections are secured regardless of the Crypto Officer role.

Note: Plaintext Cryptographic Keys and CSPs are never output from the module.

2.5.3 Access Control

Table 2.5-5 shows services from Table 2.5-4 that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)
D - The item is **deleted** by the service.

Table 2.5-5 – Access Control

Service	Authentication Data (Key or CSP)	Access Control
Authenticate Crypto Officer	RSA Public Key RSA Private Key Password	R R,E E
Load Network Certificates	RSA public and private keys RSA public key certificate System master key	W W W
Create user accounts	Password (W)	W
Modify user accounts (reset password)	Password (W)	W
Delete user accounts	Password (D)	D
Change password	Password (E,W)	E,W
Generate AES session keys	AES Session Key	W
Generate IV	IV	W
Agree on management privacy key	Management Privacy Key	W
RSA signature generation	RSA Private Key	R,E
RSA signature verification	RSA Public Key	R,E
AES encryption	Management Privacy Key Session Key	R
AES decryption	Management Privacy Key Session Key	R
Erase unit (Console Command)	System master key	W
Tamper	System master key	W
Alternating Bypass	System master key	E
Set FIPS Mode	All	W

2.6 Physical Security

The module employs the following physical security mechanisms:

The encryptor is made of commercially available, production-grade components meeting commercial specifications for power, temperature, reliability, shock and vibration.

- All integrated circuit chips have passivation techniques and materials applied to them.
- The enclosure is strong and opaque.
- Attempts to enter the module without removing the cover will cause visible damage to the module.

Access to the circuitry contained within the encryptor is restricted by the use of tamper detection and response (CSP zeroization) circuitry. Attempting the removal of the module from the enclosure causes the immediate zeroization of the 168-bit symmetric System Master Key, rendering all cryptographic keys and CSPs indecipherable. This capability is operational whether or not power is applied to the module.

Tamper-evident tape is pre-installed over the module's rear panel where the screws connect the chassis to the rear panel, providing visible evidence of any attempt to remove the chassis to obtain access to the internal components of the module.

Any attempts to remove the module cover are considered tampering; access to the cryptographically relevant components of the module requires the cover to be removed. When the module detects tampering it destroys the cryptographic keys and unprotected CSPs automatically, then returns to an uncertified state and remains in that state until it is re-certified.

If the Tamper Switch is triggered while the module is powered on:

- the module erases the 168-bit symmetric key which is used to encrypt the unit's private key and user localized passwords
- the module also erases any active key material

After tamper activation the system is uncertified and the SEC LED is illuminated red until a new certificate is loaded.

If the Tamper Switch is triggered while the module is powered off:

- the module zeroizes the 168-bit symmetric System Master Key
- the SEC LED will be illuminated red after the module is powered on

While in the uncertified state, the CLI and SNMPv3 access are still active, but no user data is output from the module. The module indicates this state with the SEC LED illuminated red on the front panel.

In addition to the physical security mechanisms integrated with the module, the following recommendation should be considered in the implementation of a Security Policy governing the installation and operation of the encryptors:

- To ensure the security of the module during distribution and delivery, the User's Guide contains procedures in the FIPS Mode Operation Guidance section for inspection of the module by an authorized operator.
- Secure access to the cryptographic module within a physically secure, limited access room or environment.

Table 2.6-1 outlines the recommended inspection and/or testing of the physical security mechanisms.

Table 2.6-1 - Security Mechanism Inspection and Test

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Switch	No direct inspection or test is required.	The module enters the tamper error state when the switch is tripped. Once in this state, the module blocks all traffic until it is physically reset.
Tamper Evidence	In accordance with organization's Security Policy.	Inspect the enclosure and tamper evident seals for physical signs of tampering or attempted access to the cryptographic module. During normal operation, the SEC LED is illuminated green. If the unit is uncertified or tampered, the SEC LED is illuminated red and all traffic is blocked.

2.7 Self Tests

In addition to the physical security mechanisms noted in 2.6, the encryptor performs both power-up and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it transitions to an error state and blocks all traffic on the data ports. Table 2.7-1 summarizes the system self tests.

Crypto Officers can run the power-up self-test on demand by issuing a reboot command. An operator with physical access to the device can also run the power-up self-test on demand by cycling the power to the module. Rebooting or power cycling the module causes the keys securing the connection to be reestablished after communications are restored.

The design of the cryptographic module ensures that all data output via the data output interface is inhibited whenever the module is in a self-test condition. Status information displaying the results of the self-tests is allowed from the status output interface, but no CSPs, plaintext data, or other information that if misused could lead to a compromise is passed to the status output interface.

Table 2.7-1 - Self Tests

Self Test	Description
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic function, performed by the encryptor, is tested using a "known answer" test to verify the operation of the function. Algorithms tested: AES, HMAC, SHS (SHA-1), Triple-DES, RNG, RSA
Firmware	The binary image(s) of the encryptor's firmware includes a 160-bit error detection code (EDC) that allows the encryptor to verify the integrity of the firmware. Each EDC is calculated for the image(s) and compared with the known value(s) to confirm the integrity of the module.
Bypass	The Connection Action Table (CAT) contains settings for bypass mode (configured administratively). Each time the CAT is changed, the system generates a checksum and stores it as a parameter. On booting, the system calculates a fresh checksum and compares it to the stored value to assure that the CAT rules have not changed or been corrupted. If the values do not match, the encryptor determines an error exists within the CAT. The encryptor sets an alarm and does not pass data (encrypted or unencrypted) to any connection. To manually confirm the bypass configuration, review the settings in the CAT. This may be accomplished with the SMC application or via the console at the encryptor. • With SMC, log into the management application and select the target encryptor from the Device table. Review device status on the Status tab or configure specific connection settings on the Security tab. Refer to the SMC documentation for details. • At the encryptor, log into the console and use the **tunnels** command (Ethernet). Refer to the device for details.
Critical Functions tests performed at power-up:	
Configuration Memory	A test to verify the configuration memory integrity. An error detection formula is calculated on all configuration memory and compared against the expected value (EDC), which is also stored in the configuration memory. If failed, the unit attempts to correct the EDC and report the failure.
Real Time Clock	The real time clock is tested for valid time and date. If this test fails, the time/date is set to 01-Jan-2000 at 00:00.

Self Test	Description
Battery	The battery is tested to determine if it is critically low. This test is guaranteed to fail prior to the battery voltage falling below the minimum specified data retention voltage for the associated battery-backed components. If this test should fail, the battery low alarm condition will be on. The unit will continue to operate after taking whatever precautions are necessary to guarantee correct operation. Battery replacement is performed by a SafeNet technician.
General Purpose Memory	A destructive test verifies that the general purpose memory (RAM) is properly operating, e.g., all legal addresses may be written to and read from, and that no address lines are open or shorted.
Tamper Memory	Tamper memory is examined for evidence of Tamper.
Conditional tests performed, as needed, during operation:	
Pairwise consistency	Public and private keys are used for the calculation and verification of digital signatures and also for key transport. Keys are tested for consistency, according to their purpose, at the time they are generated. Encryption keys are tested by an encrypt/decrypt pairwise consistency test while signature keys are tested by a sign/verify pairwise consistency test. Algorithms tested: RSA
Firmware load	Test to verify the authenticity of any software/firmware load that is applied to the Encryptor in the field. The software/firmware RSA signature is verified.
Continuous RNG	This test is a “stuck at” test to check the RNG output data for failure to a constant value. All internal RNGs are subject to this test.

3 Glossary of Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CAT	Connection Action Table
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed) Hash Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MIB	Management Information Base
MPK	Management Privacy Key
MSK	Master Session Key
NC	Network Certificate
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comment
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman (public key algorithm)
SHA	Secure Hash Algorithm
SK	Session Key
SMC	Security Management Center
SMK	System Master Key
SNMPv3	Simple Network Management Protocol version 3
SEE BO	SafeNet Ethernet Encryptor Branch Office
X.509	Digital Certificate Standard RFC 2459