# SafeEnterprise[TM] Encryptor

# Model 650 for 10 Gigabit Networks

# FIPS 140-2 – Overall Level 2 Validation Non-Proprietary Security Policy



## Hardware Part Number

| 10 GB | (904-200xx-00y) | 904-210xx-00y (RoHS) |
|-------|-----------------|----------------------|

with

**3.1 Firmware**

**Security Policy Revision 1.02**
**May 21, 2008**

# 1    Introduction

This document is the Security Policy for the SafeEnterprise<sup>TM</sup> Encryptor model 650 (also referred to in this document as the encryptor) 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 and 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 SafeEnterprise<sup>TM</sup> Encryptor 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/CSE 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 Program, can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html. More information describing the SafeEnterprise<sup>TM</sup> Encryptor can be found at http://safenet-inc.com.

In this document, the SafeEnterprise<sup>TM</sup> Encryptor is also referred to as "the module" or "the encryptor".

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.

The SafeEnterprise<sup>TM</sup> Encryptor (the module) meets the overall requirements applicable for FIPS 140-2 Level 2 security with selected Level 3 requirements as listed in Table 1.

**Table 1. Cryptographic Module Security Requirements**

| *Security Requirements Section* | *Level* |
|---|---|
| **Cryptographic Module Specification** | 2 |
| **Cryptographic Module Ports and Interfaces** | 3 |
| **Roles and Services and Authentication** | 3 |
| **Finite State Machine Model** | 2 |
| **Physical Security** | 3 |
| **Operational Environment** | N/A |
| **Cryptographic Key Management** | 3 |
| **EMI/EMC** | 2 |
| **Self-Tests** | 2 |
| **Design Assurance** | 3 |
| **Mitigation of Other Attacks** | N/A |
| **Cryptographic Module Security Policy** | 2 |

## 1.1    Acronyms and Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ATM | Asynchronous Transfer Mode |
| 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 Block |
| 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-1 | Secure Hash Algorithm |
| SMC | Security Management Center |
| SNMPv3 | Simple Network Management Protocol version 3 |
| VCAT | Virtual Channel Action Table |
| X.509 | Digital Certificate Standard RFC 2459 |

## 2      SafeEnterprise<sup>TM</sup> Encryptor

### 2.1     Functional Overview

The SafeEnterprise<sup>TM</sup> Encryptor provides data privacy and access control for connections between vulnerable public and private networks. It employs FIPS-approved AES and Triple-DES algorithms and can be deployed in 10 Gigabit (OC-192) networks. The encryptor can be centrally controlled or managed using SafeNet's SafeEnterprise Security Management Center (SMC), an SNMPv3-based security management system.

The role of the encryptor is illustrated in Figure 1. The encryptor is installed between private network equipment such as a switch or add-drop multiplexer and a public network. The encryptors communicate in pairs in the network, establishing secured connections between the 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. The encryptor has dual, hot swap -48V DC power supplies.

**Figure 1. Encryptor Operation.**
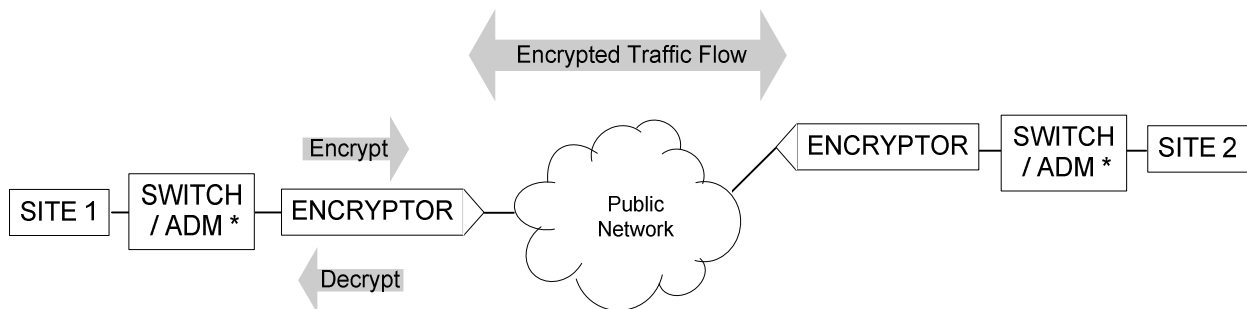


  * ADM = Add/Drop Multiplexer

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

Figure 2 shows an example of two secured sessions between sites.

To negotiate a session key value and maintain encryption synchronization, the encryptor utilizes one overhead byte that must be passed by the network between encryptors. The specific overhead byte used depends on the network layer that the encryptor is configured to encrypt.

Some overhead bytes are required to be passed unmodified or regenerated in order for network equipment to properly handle the frame, therefore the encryptor automatically bypasses data in these overhead bytes. The remaining overhead bytes are handled as specified by the user when the secure session is configured.  The user may choose to encrypt overhead bytes, pass overhead bytes unmodified, or zeroize overhead bytes.

**Figure 2. Encryptor Usage Example.**
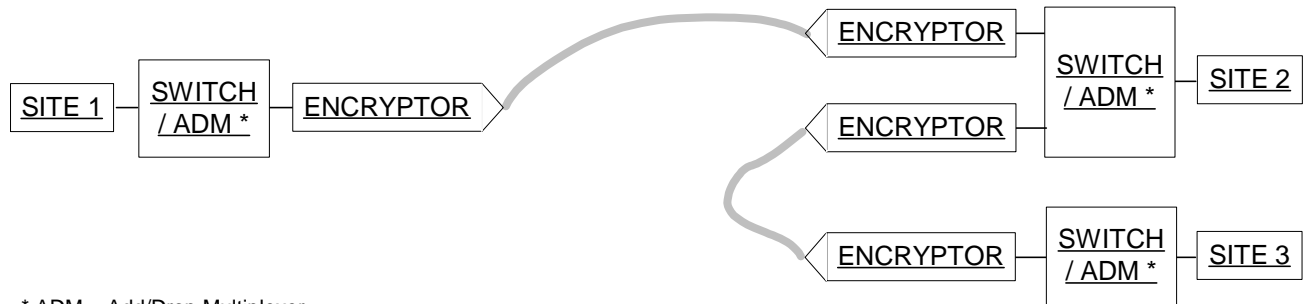


* ADM = Add/Drop Multiplexer

## *2.2   Module Description*

The SafeEnterprise[TM] Encryptor 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 steel case completely encloses the encryptor to protect it from tampering. Any attempt to remove the cover will automatically erase all sensitive information stored internally in the encryptor.

> **Note:** The -48V DC power supplies are outside the cryptographic boundary. The case is designed to prevent tampering or probing of the internal components even when the power supplies are removed.

The encryptor provides data privacy and access control services for networks utilizing 10 Gigabit (OC-192) communications. The SafeEnterprise[TM] Encryptor supports a single path or line.

The module supports pluggable transceiver options to handle speed and distance variants. The transceivers are outside the cryptographic boundary.

Note: The Hardware Part Number includes options for pluggable transceivers (shown as 'xx' ) and power cords  (shown as 'y'). A representative part number for an encryptor with 1310nm (10km) transceivers and pigtail -48vdc power cord would be 904-20044-004.

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

All 650 series models share a common enclosure. The following figure shows the front view, which is the same for both the 650 series models. The front panel provides a network management port, a console port, a USB port, an LCD display and LEDs for status, and a keypad for control input. The height accommodates the dual -48V DC power supplies.

**Figure 4. Model 650 Encryptor Front View.**



The Model 650 encryptor has two network interfaces located in the back of the module: the Local Port interface connects to a physically secure private network and the Network Port interface connects to an unsecure public network. The rear panel also contains a tamper evident seal that indicates movement of the module cover with respect to the module enclosure.

**Figure 5. Model 650 Encryptor Rear View**



.

The module has eight physical ports and four logical interfaces. The physical ports have the following functions:

- Front Panel **RJ45** Ethernet port allows remote management from the SMC application. Access is protected by IPSec security mechanisms for authentication and data encryption.

- Front Panel 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 front panel **USB port** is reserved for future use.

- The rear panel **power connectors** are used for power input to the module. DC power can be -40V DC to -72V DC.

- The **Network Port** connects to the public network via the transceiver's rear panel public network 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 transceiver's rear panel local network connector . The Local Port and Network Port are of the same interface type.

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

**Table 3. Cryptographic Module Logical Interfaces**

| Logical Interface | Description |
|---|---|
| Data Input Data Output | Local Port: <br><br>• Connects to the private network via the transceiver, sending and receiving plaintext user data. <br><br>Network Port: <br><br>• Connects to the public network via the transceiver, sending and receiving ciphertext and plaintext user data to and from a far end module. <br><br>• Sends authentication data and RSA key exchange components to a far end module. <br><br>• Receives authentication data, RSA key exchange components from a far end module. <br><br>• The module can be set to bypass, to send and receive plaintext for the selected connection. |
| Control Input | Control Input is provided by the front panel keypad, the serial port, the RJ45 and the Local and Network ports (via their respective transceiver) as follows: <br><br>• The front panel keypad is used for initialization prior to authentication and operation in the approved mode. An operator uses the keypad to set the IP address for remote administration by SMC, set the system clock and load the certificate (in conjunction with the SMC). <br><br>• The front panel DB9 RS-232 serial console port may be used for initialization prior to authentication and operation in the approved mode as an alternative to using the keypad. This port receives control input (protected via a username and password) from a locally connected terminal. <br><br>• The front panel RJ45 Ethernet port receives out-of-band control input from the SMC application. <br><br>• Local and Network ports may receive in-band control input (via their respective transceiver), protected via the SNMPv3 security mechanisms, from the SMC application. |
| Status output | Status output is provided by the front panel LEDs, the Front Panel DB9 RS-232 port, the Ethernet Port (out-of-band status), and the Local and Network ports (in-band status) as follows: <br><br>• Front panel LEDs indicate the state of RSA keys and certificates, error states, state of the local and network interfaces, alarm, temperature, and battery state. <br><br>• The front panel DB9 RS-232 serial console port may be used for initialization prior to authentication and operation in the approved mode as an alternative to using the keypad. It is also used for monitoring some operations. This port sends status output (protected via a username and password) to a locally connected terminal. <br><br>• The front panel RJ46 Ethernet port sends out-of-band status output information to an SMC application. |

| Logical Interface | Description |
|---|---|
|  | • Local and Network ports may send in-band status output information (via their respective transceiver), protected via the SNMPv3 security mechanisms, to the SMC application. |

The following table maps FIPS 140-2 logical interfaces to the cryptographic module's logical interface and physical port.

**Table 4. Logical interface to Physical Port Map**

| FIPS 140-2 Logical Interface | Logical Interface | Physical Port |
|---|---|---|
| Data Input | 1) Public network interface<br>2) Private network interface | 1) Network port transceiver connector<br>2) Local port transceiver connector |
| Data Output | 1) Public network interface<br>2) Private network interface | 1) Network port transceiver connector<br>2) Local port transceiver connector |
| Control Input | 1) SNMPv3 interface<br>2) Local console<br>3) Keypad<br>4) Public network interface<br>5) Private network interface | 1) Front Panel RJ45 Ethernet port<br>2) Front Panel DB9 RS-232 serial console port,<br>3) Front Panel Keypad/Display<br>4) Rear panel Network Port<br>5) Rear panel local port |
| Status Output | 1) SNMPv3 interface<br>2) Local console<br>3) Front Panel Display | 1) Front Panel RJ45 Ethernet port<br>2) Front Panel DB9 RS-232 serial console port,<br>3) Front Panel LED Display |
| 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. The module separates these two logically distinct categories of information, using the network protocol that treats all overhead bytes as control or status data.

## 2.3   Security Functions

The module provides symmetric key encryption (Triple-DES or AES) for user data transferred through the module. Asymmetric keys and SHA-1 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-1 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 5. Module Algorithms.**

| Approved Algorithm | Certificate | | |
|---|---|---|---|
| | *Encryptor* | *Cryptolib* | *QuickSec* |
| **AES (FIPS PUB 197)** ECB(e only; 256); CTR(int only; 256) CBC(e/d; 256) | 391 | | 240 |
| **Triple-DES (FIPS PUB 46-3)** TCFB8 (e/d; KO 1,2,3) | | 268 | |
| **Hashing** SHA-1 byte-oriented hashing HMAC SHA-1 | | 251 | 319 48 |
| **Random Number Generation** ANSI X9.31 | | 18 | 76 |
| **Digital Signatures** Key Gen ANSI X9.31 / Sig Gen PKCS#1/ Sig Ver PKCS#1 \| 1024 \| SHA-1 | | 15 | |

The encryptor implements the following security functions:

**Table 6. Module Security Functions.**

| Security Function |
|---|
| **Symmetric Key Encryption** AES Triple-DES |
| **Key Establishment** RSA key establishment (per ATM Forum Security Spec 1.1) |
| **Key Agreement** Diffie-Hellman Key Agreement |
| **Authentication** RSA asymmetric key 1024 bit (per ANSI X9.31) HMAC SHA-1 |
| **Key Generation** Triple-DES/AES Keys – PRNG (per ANSI X9.31) |

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

## 2.4 FIPS Approved Mode of Operation

In the FIPS approved mode of operation, 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.

The module is specifically configured such that its only operational mode is the FIPS approved mode. A Crypto officer must still ensure the cryptographic module operates in the FIPS approved mode. Crypto officers can view the module front panel Secure LED that is steady green when the module is in FIPS mode. FIPS mode status may also be queried from the management application. Operators may run the power-on self test on-demand by power-cycling the module.

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 Network Certificates in digitally signed messages. The module cannot build a secure connection with a remote module that does not have a valid Network Certificate. Moreover, the module cannot establish any connections connection unless it has been issued a valid NC. This mode of operation requires a common Security Management Center to issue Network Certificates 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 negotiated Triple-DES or 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.

## 2.5 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 7:

**Table 7. Roles and 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. While only one operator may be connected via the console at a time, multiple concurrent IPSec sessions are permitted. While the IPSec connections are session oriented, the SNMPv3 based management, within each IPSec session, is not session oriented; thus, multiple operators could be issuing SNMPv3 commands with each command processed individually as it is received by the encryptor. Similarly, 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. Operators (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 IPSec based authentication establish a secure connection, or 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 by a Crypto Officer before the module is returned to the factory, either by command or by removing the network interface card(s).

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

**Table 8. Strength of Authentication.**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| **Authentication Password** | Crypto Officers accessing the CM using the CLI (via the console port) must authenticate, using a password that is at least 8 characters and at most 16 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 14.7 million) possible combinations; 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.<br><br>Note: the module also suppresses feedback of authentication data being entered into the CLI by returning blank characters. |
| **Authentication from SMC** | Authentication with SMC is accomplished via IPSec and a pre-shared secret. The pre-shared secret is a 2048-byte passphrase based on the ASCII character set. Based on a 2048-byte secret, 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 passphrase 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 1024-bit key. 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 1/100,000. The multi-step handshaking process for establishing a |

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| | 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

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) employed within the module.

**Table 9. 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 (3-key Triple-DES CBC) the module's public and private RSA keys and the user table stored in the configuration flash memory.<br><br>On tamper, the module zeroizes system master key rendering encrypted data in 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. This key is used to authenticate sessions with other encryptors and to unwrap master session keys and session keys received from far-end encryptors. The key is stored in 3-key Triple-DES-encrypted format in Flash memory. On tamper, the Triple-DES system master encryption key is zeroized, rendering the encrypted private key undecipherable. |
| RSA Public Key | The public component of the module's RSA Key pair is stored in 3-key Triple-DES-encrypted format in Flash memory. It also resides in the Network Certificate that is stored in the clear in system non-volatile RAM and is used for authenticating connections with other encryptors. On tamper, the Triple-DES system master encryption key is zeroized, rendering the encrypted public key undecipherable. |
| 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).<br><br>The CLI uses the authentication password to authenticate Crypto Officers accessing the system via the console port.<br><br>SNMPv3 concatenates and hashes (SHA1) 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.<br><br>Passwords and usernames are hashed and stored in the user table in 3-key Triple-DES-encrypted format in Flash memory. On tamper, the Triple-DES system master encryption key is zeroized, rendering the encrypted passwords undecipherable. |
| Privacy Password | The Privacy Password is an unused artifact of SNMPv3. Since it is maintained within the module, any assigned Privacy Password is protected along with the rest of the keys and CSPs. |

| Data Item | Description |
|---|---|
| | The Privacy Password is stored in 3-key Triple-DES-encrypted format in Flash memory. On tamper, the Triple-DES system master encryption key is zeroized, rendering the encrypted HMAC key undecipherable. |
| **IPSec Passphrase Secret** | The 2048-byte IPSec Passphrase Secret authenticates an operator (SMC) attempting to establish a remote session with the module. The IPSec Passphrase Secret acts as a shared secret between the management station and the module. Once authenticated, Diffie-Hellman key agreement is used to establish the Session Keys that are used to secure the management traffic. |
| **Session Master Key** | For each session, the module generates a symmetric session master key (and other session keys) via the ANSI X9.31 PRNG, and uses RSA key exchange to transfer these keys to a far-end encryptor for data encryption and decryption purposes. The session master key persists for the life of the session and is used to (AES or Triple-DES) encrypt session keys that may be changed periodically during the session. All session keys are destroyed at the end of a session. |
| **Session Keys** | For each session, the module generates a symmetric session master key and two session keys for each data flow path in a secure connection (one for the Initiator-Responder path and another for the Responder-Initiator path). These keys AES encrypt user data transferred between encryptors. Session keys may be changed periodically during the session based on time or based on the amount of data transferred. All session keys are destroyed at the end of a session. |
| **Network Certificate** | The X.509v3 certificate that is associated with the encryptor in an operational environment. It is produced and signed by the managing SMC system. The certificate is stored in the clear in system Non-volatile system RAM and used for authenticating connections with other encryptors. Other encryptors use the embedded public key to wrap initial session keys to Triple-DES or AES encrypt a session. The certificate is deleted from memory only on an Erase command from a module operator or a tamper condition. |

*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 certificate has been properly loaded into the module. The module also prevents data output during and after zeroization of cryptographic keys and CSPs as this occurs when a tamper condition exists. Further, the system'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 10 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 10. 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 | | ● | | |
| Modify IPSec Passphrase | | ● | | |
| Show Software Version | | ● | ● | |
| View User Accounts | | ● | ● | |
| Clear Audit Trail | | ● | | |
| View Audit Trail | | ● | ● | |
| Clear Event Log | | ● | | |
| View Event Log | | ● | ● | |
| View FIPS Mode Status | | ● | ● | |
| Run Self Test (Power Cycle the Module) | ● | | | |
| Run Self Test (Reboot Command) | | ● | | |
| Generate AES session keys | | ●[1] | | ● |
| Generate Initialization Vector | | ●[1] | | ● |
| RSA signature generation | | ●[1] | | ● |
| RSA signature verification | | ●[1] | | ● |

| Service | No Role | Crypto Officer (Full Access) | Crypto Officer (Read Only) | Network User |
|---|---|---|---|---|
| AES encryption | | ● [2] | | ● |
| AES decryption | | | | ● |
| Triple-DES encryption and decryption (for the master secret) | | ● | | |
| SHA-1 Hashing for password verification | ● | | | |
| Generate DH keys | | | | ● |
| DH Key Agreement | | ● [1] | | ● |
| Software/firmware load test | | ● | | |
| Erase unit (Console Command) | | ● | | |
| Tamper | ● | | | |

[1] Restarting a connection causes new session keys to be generated.

[2] Plaintext data entering the Local port is encrypted if the connection is set to encrypt data.

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

### 2.5.3   Access Control

Table 11 shows services, from Table 10 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 11. Access Control

| Service | Authentication Data (Key or CSP) | Access Control |
|---|---|---|
| Authenticate Crypto Officer | RSA Public Key<br>RSA Private Key<br>or Password | R<br>R,E<br>E |
| Load Network Certificates | RSA public and private keys<br>RSA public key certificate<br>System master key | W<br>W<br>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 |
| Modify IPSec passphrase | IPSec passphrase | W |
| Generate AES session keys | AES Session Key | W |

| Service | Authentication Data (Key or CSP) | Access Control |
|---|---|---|
| Generate IV | IV | W |
| RSA signature generation | RSA Private Key | R,E |
| RSA signature verification | RSA Public Key | R,E |
| AES encryption | Session Key | R |
| AES decryption | Session Key | R |
| Erase unit (Console Command) | System master key | W |
| Tamper | System master key | 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 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. Ventilation holes on the side of the unit are fitted with baffles, or other obscuring material, to prevent undetected physical probing inside the enclosure.

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 enclosure's cover 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 interface module face plates. The tamper evident tape provides visible evidence of any attempt to remove the interface cards 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. Removal of the cover requires removal of the network interface cards which triggers the Tamper Switch. If the module detects tampering it destroys the cryptographic keys and unprotected critical security parameters automatically. The module 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. It will also erase any active key material and log an event message indicating that the card has been removed. After tamper activation the system is uncertified and the Secure LED is illuminated red until a new certificate is loaded. If the Tamper Switch is triggered while the module is powered off, the module erases the 168-bit symmetric System Master Key. The event message will be logged and the Secure 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 Secure 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:

- Secure access to the cryptographic module within a physically secure, limited access room or environment.

Table 12 outlines the recommended inspection and/or testing of the physical security mechanisms.

**Table 12. 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 tape for physical signs of tampering or attempted access to the cryptographic module. During normal operation, the Secure LED is illuminated green. If the unit is uncertified or tampered, the Secure LED is illuminated red and all traffic is blocked. |

## 2.7    Self Tests

In addition to the physical security mechanisms noted above, 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 13 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 13. 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. |
| **Software/Firmware** | The binary image(s) of the encryptor's firmware includes a 16-bit error detection code (EDC) that allows the encryptor to verify the integrity of the firmware. The EDC is calculated for the image(s) and compared with the known value(s), using a SHA-1 hash, to confirm the integrity of the module. |
| **Bypass** | The session table contains settings for bypass mode (configured administratively). Each time the session table 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 session table rules have not changed or been corrupted. If the values do not match, the encryptor determines an error exists within the session table. The encryptor sets an alarm and does not pass data (encrypted or unencrypted) to any session. |
| **Critical Functions tests performed at power-up:** | |

| Self Test | Description |
|---|---|
| **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-1996 at 00:00. |
| **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. |
| **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. |
| **Software/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   References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.