SafeEnterprise™ ATM Encryptor II
Model 600
FIPS 140-2 – Level 3 Validation
Non-Proprietary Security Policy

Hardware Models

T1 RJ45	(901-11001-00x)
E1 BNC	(901-27001-00x)
T3 BNC	(901-37001-00x)
E3 BNC	(901-77001-00x)
OC-3/STM1 Multi-Mode	(901-41001-00x)
OC-3/STM1 Single Mode	(901-61001-00x)
OC-12/STM4 Multi-Mode	(901-51001-00x)
OC-12/STM4 Single Mode	(901-81001-00x)

with

3.0 Firmware

Security Policy Revision 1.0
December, 2005

1 Introduction

This document is the Security Policy for the SafeEnterprise™ ATM Encryptor II, Model 600, 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 SafeEnterprise™ ATM Encryptor II 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 Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. 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 CMV Program, can be found at http://csrc.nist.gov/cryptval. More information describing the SafeEnterprise™ ATM Encryptor II can be found at http://safenet-inc.com.

In this document, the SafeEnterprise™ ATM Encryptor II is also referred to as “the module” or “the encryptor”. This Security Policy defines the cryptographic module for multiple models of SafeEnterprise™ ATM Encryptor II product consisting of ATM variants from T1 to OC-12. These models are functionally identical except for the network interface.

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™ ATM Encryptor II (the module) meets the overall requirements applicable to Level 3 security for FIPS 140-2.

Table 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

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
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
RAM	Random Access Memory
RFC	Request for Comment
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SDH	Synchronous Digital Hierarchy
SHA-1	Secure Hash Algorithm
SMC	Security Management Center
SNMPv3	Simple Network Management Protocol version 3
SONET	Synchronous Optical Network
VCAT	Virtual Channel Action Table
VPI/VCI	Virtual Path Identifier/Virtual Channel Identifier
X.509	Digital Certificate Standard RFC 2459

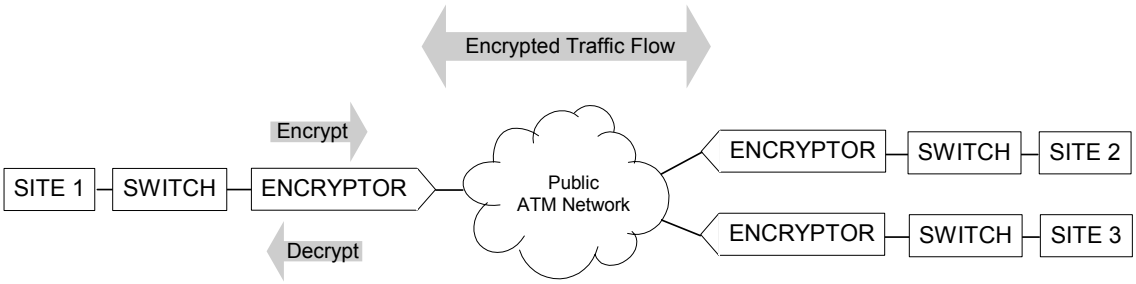
2 SafeEnterprise™ ATM Encryptor II

2.1 Functional Overview

The SafeEnterprise™ ATM Encryptor II provides data privacy and access control for connections between vulnerable public and private ATM networks. It employs federally endorsed AES and Triple-DES algorithms and, with the flexibility to choose the desired interface module, can be deployed in ATM T1, E1, T3, E3, OC-3c and OC-12c networks. The encryptor can be centrally controlled or managed across multiple remote stations 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 an ATM switch and an ATM network. An encryptor communicates with other encryptors in the network, establishing secured connections between itself and the other modules. The encryptors selectively encrypt, reject, 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.

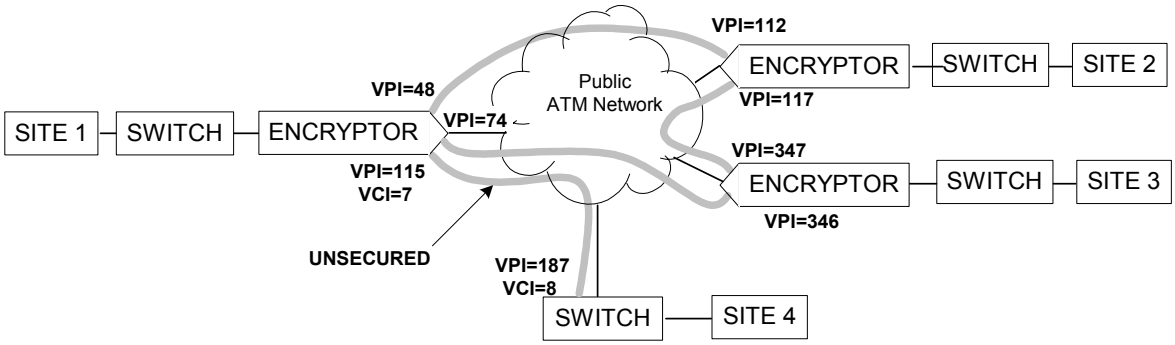
Figure 1. Encryptor Operation.



Secured connections are established between the cryptographic module and similar units using the RSA key exchange process. This results in a separate secure link per path or channel connection and does not require any secret connection keys to ever be displayed or manually transported and installed.

The encryptor supports Permanent Virtual Paths (PVPs) and Permanent Virtual Channels (PVCs). Figure 2 shows an example of three secured connections and one unsecured connection between sites. A secured connection is based on a VPI (Virtual Path Identifier), and VCI (Virtual Channel Identifier), so it is possible to have multiple secured connections between two secure units. Since the network can change the value of the VPIs and VCIs, the values at each end of a secure connection are usually different. In the example below there are 3 secured connections: VPI 48-112, 74-346, and 117-347. Connection VPI/VCI 115/7-187/8 is unsecured because a SWITCH (ATM access device), by itself, cannot handle encrypted traffic. This connection is configured to transfer data as plaintext. VCI connections 0-31 default to plaintext since they are reserved for management traffic.

Figure 2. Encryptor Usage Example.



2.2 Module Description

The SafeEnterprise™ ATM Encryptor II 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.

The encryptor provides data privacy and access control services for ATM networks, supporting up to 256 virtual paths, 1024 virtual channels or a combination of paths and channels. The encryptor can be deployed in ATM networks utilizing T1, E1, T3, E3, OC-3c and OC-12c communications. There are 8 basic FIPS 140-2 validated models of the SafeEnterprise™ ATM Encryptor II, Model 600, running the 3.0 firmware release. The systems employ one of two functionally equivalent cryptographic acceleration modules depending on the speed of the interface.

Table 2. Supported Models

Model	*Supported Interface*	*Acceleration Module*
901-11001-00x	T1 RJ45	Crypto-155 Module
901-27001-00x	E1 BNC	Crypto-155 Module
901-37001-00x	T3 BNC	Crypto-155 Module
901-77001-00x	E3 BNC	Crypto-155 Module
901-41001-00x	OC-3/STM1 Multi-Mode	Crypto-155 Module
901-61001-00x	OC-3/STM1 Single Mode	Crypto-155 Module
901-51001-00x	OC-12/STM4 Multi-Mode	Crypto-622 Module
901-71001-00x	OC-12/STM4 Single Mode	Crypto-622 Module

The ‘x’ in the model numbers represents the variants; where ‘x’ may be:

- 1 US power cord
- 2 UK power cord
- 4 European power cord
- 5 Swiss power cord
- 7 -48V DC power

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 models share a common enclosure. The following figure shows the front view, which is the same for all the models except for the labeling. 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.

Figure 3. Encryptor Front View.

The 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. While the rear view is similar for the various models, it is interface specific as illustrated in the following sample figures. The rear panel also contains the power connector (US 120v connector shown), the power switch, and a tamper evident seal that indicates movement of the module cover with respect to the module enclosure.

Figure 4. Encryptor Rear View (RJ-45 Connectors)

Figure 5. Encryptor Rear View (BNC Connectors)

Figure 6. Encryptor Rear View (Optical Connectors)

2.3 Module Ports and Interfaces

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. In a future release it may provide a mechanism for applying appropriately signed and secured updates to the system. Current system software provides no ability to access the system or output data via this port.

- The rear panel **power connector** is used for power input to the module. AC power can be 100 - 230 VAC, 47-63 Hz nominal frequencies. DC power can be -40 to -72 VDC.
- The rear panel **Network Port** connects to the public network. The interface can be T1, E1, T3, E3, OC-3c, OC-12c, or OC-48. Access is protected by RSA certificates. The Local Port and Network Port are of the same interface type.
- The rear panel **Local Port** connects to the private network. The interface can be T1, E1, T3, E3, OC-3c, OC-12c, or OC-48. 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: • Connects to the private network, sending and receiving plaintext user data. Network Port: • Connects to the public network, 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 selected VPI/VCI connections.
Control Input	Control Input is provided by the front panel keypad, the serial port, the RJ45 and the Local and Network ports as follows: • 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). • 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. • The front panel RJ45 Ethernet port receives out-of-band control input from the SMC application. • 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 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: • 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.

Logical Interface	*Description*
	• 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. • The front panel RJ46 Ethernet port sends out-of-band status output information to an SMC application. • Local and Network ports may send in-band status output information, 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 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) Keypad 4) Public network interface 5) Private network interface	1) Front Panel RJ45 Ethernet port 2) Front Panel DB9 RS-232 serial console port, 3) Front Panel Keypad/Display 4) Rear panel Network Port 5) Rear panel local port
Status Output	1) SNMPv3 interface 2) Local console 3) Front Panel Display	1) Front Panel RJ45 Ethernet port 2) Front Panel DB9 RS-232 serial console port, 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 (Operation and Maintenance (OAM) cells or special network cells) and user data enter, and exit, the module over the network port. The module separates these two logically distinct categories of information, using the ATM protocol that treats all cells with a VCI address of 31 or lower, as control or status data cells.

2.4 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*			
	Crypto-155	*Crypto-622*	*Cryptolib*	*QuickSec*
AES (FIPS PUB 197)				
CFB128 (e/d; 256)	166	167		
CBC (e/d; 256)				240
Triple-DES (FIPS PUB 46-3)				
TECB (e only; KO 1,2,3) ; CTR (int only; KO 1,2,3);	269	270		
TCFB64 (e/d; KO 1,2,3)	269	270	268	
TCFB8 (e/d; KO 1,2,3)				
Hashing				
SHA-1 byte-oriented hashing			251	319
HMAC SHA-1				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
Symmetric Key Establishment (See Note below this table)
RSA key wrapping (per ATM Forum Security Spec 1.1)
Diffie-Hellman key agreement
Authentication
RSA asymmetric key 1024 bit (per ANSI X9.31)
HMAC SHA-1

Security Function
Key Generation Triple-DES/AES keys – PRNG (per ANSI X9.31) RSA keys – ANSI X9.31

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

2.5 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.

2.6 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).

Role	*Type of Authentication*	*Authentication Data*
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. When interacting with legacy module Network Users, a 16-byte Crypto Passphrase Key is presented for authentication purposes as outlined below.

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 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 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.

Authentication Mechanism	*Strength of Mechanism*
	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 either 1024-bit RSA authentication or a signed Crypto Certificate (specified below). 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. Similarly, the 16-byte Crypto Passphrase Key, used with the Crypto Certificate, is a hashed message digest based on the 2048-byte Interoperability Passphrase Secret concatenated with an internal 8-byte “salt” value, 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 sets the possibility of randomly guessing the authentication data in 60 seconds at less than 1 in 100,000.

2.6.1 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. 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 PVPs and PVCs 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

Data Item	*Description*
	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). The CLI uses the authentication password to authenticate Crypto Officers accessing the system via the console port. 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. 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. 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.
Interoperability Passphrase Secret (also referred to as the Passphrase)	There is a single 2048-byte Interoperability Passphrase Secret that may be established within the module. The Interoperability Passphrase Secret is a shared secret, and is used in the generation of the Crypto Certificate and its associated Crypto Passphrase Key. The Crypto Certificate is used for authentication with legacy SafeEnterprise ATM Encryptor modules. Before the module can establish a secure connection with a far end SAE module, the two systems must authenticate using a Crypto Certificate incorporating the Crypto Passphrase Key.
Crypto Passphrase Key	The 16-byte key created during initialization using the Interoperability Passphrase Secret. It is used to create an authentication signature for the Crypto Certificate and to authenticate Crypto Certificates received from a far-end ATM Encryptor system. The Interoperability Passphrase Secret, entered during initialization, is converted to a key using a cryptographically strong message digest algorithm. The cleartext passphrase is concatenated with an 8-byte, SafeNet supplied, “salt” value, and hashed, creating the Crypto Passphrase Key. Note: The Crypto Passphrase Key is used for authentication, but not for encryption purposes.
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.
Key Exchange Key	A key generated when initially authenticating (and conversing) with a legacy ATM Encryptor. Once a pair of encryptors has mutually authenticated, they cache the Key Exchange Key, so that subsequent exchanges between the encryptors re-use the

Data Item	*Description*
	generated Key Exchange Key. The initial authentication between encryptors, when no Key Exchange Key exists, is completed using Diffie-Hellman. Since this is a relatively expensive operation, the caching of the Key Exchange Key allows all subsequent exchanges between known encryptors to be completed very efficiently. For legacy ATM interactions, the Key Exchange Key protects the transfer of the Session Master Key, which protects the transfer of subsequent Session Keys.
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 or Triple-DES 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 SAE 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.
Crypto Certificate	The proprietary certificate that is associated with the SAE for interoperability an operational environment with legacy ATM systems. It is produced and signed internally based on the Interoperability Passphrase Secret and an internal “salt” value. The certificate is stored in the clear in system Non-volatile system RAM and used for authenticating connections with legacy encryptors. Other encryptors use the embedded information to authenticate and generate the Key Exchange Key defined above. 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.

2.6.2 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 Passphrase		●		
Modify IPSec Passphrase		●		
Show Software Version		●	●	
View User Accounts		●	●	
Clear Audit Trail		●		
View Audit Trail		●	●	
Clear Event Log		●		
View Event Log		●	●	

Service	*No Role*	*Crypto Officer (Full Access)*	*Crypto Officer (Read Only)*	*Network User*
View FIPS Mode Status		●	●	
Run Self Test (Power Cycle the Module)	●			
Run Self Test (Reboot Command)		●		
Generate AES or Triple-DES session keys		● [1]		●
Generate Initialization Vector		● [1]		●
RSA signature generation		● [1]		●
RSA signature verification		● [1]		●
AES or Triple-DES encryption	● [2]			●
AES or Triple-DES decryption				●
SHA-1 Hashing for password verification	●			
Generate DH keys		● [1]		●
DH Key Agreement		● [1]		●
Erase unit (Console Command)		●		
Tamper	●			

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

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

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

2.6.3 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 RSA Private Key or Password	R R,E E

Service	Authentication Data (Key or CSP)	Access Control
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
Modify passphrase	Passphrase	W
Modify IPSec passphrase	IPSec passphrase	W
Generate AES or Triple-DES session keys	AES, Triple-DES, Session Key	W
Generate IV	IV	W
RSA signature generation	RSA Private Key	R,E
RSA signature verification	RSA Public Key	R,E
AES or Triple-DES encryption	Session Key	R
AES or Triple-DES decryption	Session Key	R
Erase unit (Console Command)	System master key	W
Tamper	System master key	W

2.7 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.

2.8 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 VPI/VCI connections 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 images of the encryptor's firmware include a 20-byte SHA-1 hash for the Error Detection Code (EDC) that allows the encryptor to verify the integrity of the firmware. The EDC is calculated for the images and compared with the known values to confirm the integrity of the module.
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.
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://www.nist.gov/cmvp.

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

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

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

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

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://www.nist.gov/cmvp.

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

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

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

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