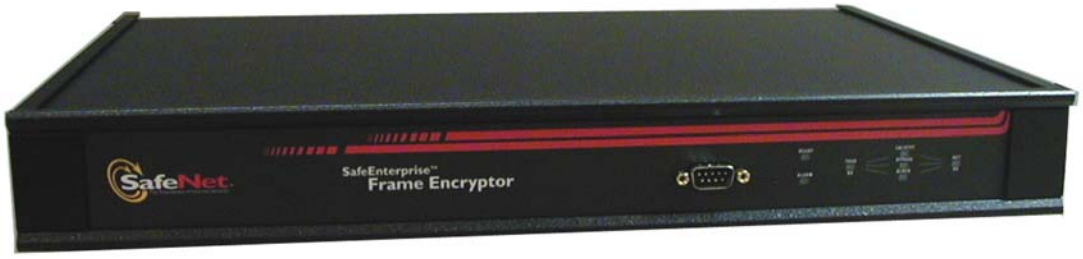
SafeNet
The Foundation of Internet Security

SafeEnterprise™ Frame Encryptor

The Foundation of Internet Security

Security Policy

SafeEnterprise™ Frame Encryptor
FIPS 140-2 - Level 3 Validation
Non-Proprietary Security Policy
(14976-3 revision 1.0)



Hardware Models

SFE Low Speed	(SE-SFE-LixAC)
SFE High Speed	(SE-SFE-HixAC
SFE HSSI	(SE-SFE-VVxAC)

with

5.00 Firmware

1 Introduction

This document is the Security Policy for the SafeEnterprise™ Frame 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 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 Frame 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 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™ Frame Encryptor can be found at http://safenet-inc.com.

In this document, the SafeEnterprise™ Frame Encryptor is also referred to as “the module”, “the encryptor”, “the Frame Encryptor” and “SFE”. This Security Policy defines the cryptographic module for three models of frame encryptor products consisting of the SFE Low Speed, High Speed, and HSSI. These models are functionally identical except for the network interface and some additional non-security relevant circuitry in the SFE-HSSI.

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™ Frame Encryptor 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	3
Cryptographic Module Security Policy	3

1.1 Document History

Table 2. Document Version

Version	Date	Comments	Name
0.01	10/24/03	Initial Draft	Ward Rosenberry
0.02	11/7/03	Initial Submission Draft	Ward Rosenberry
0.03	12/19/03	Submit to NIST	Ward Rosenberry
1.0	04/16/04	Address NIST / CSE comments	J. Vohwinkel

1.2 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DLCI	Data Link Connection Identifier
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FRAD	Frame Relay Access Device
HSSI	High-Speed Serial Interface
IP	Internet Protocol
LED	Light Emitting Diode
MC	Manufacturing Certificate
NC	Network Certificate
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Algorithm
SCA	SafeNet Certification Authority
SFE	SafeEnterprise™ Frame Encryptor
SHA	Secure Hash Algorithm
SMC	Security Management Center
SNMP	Simple Network Management Protocol

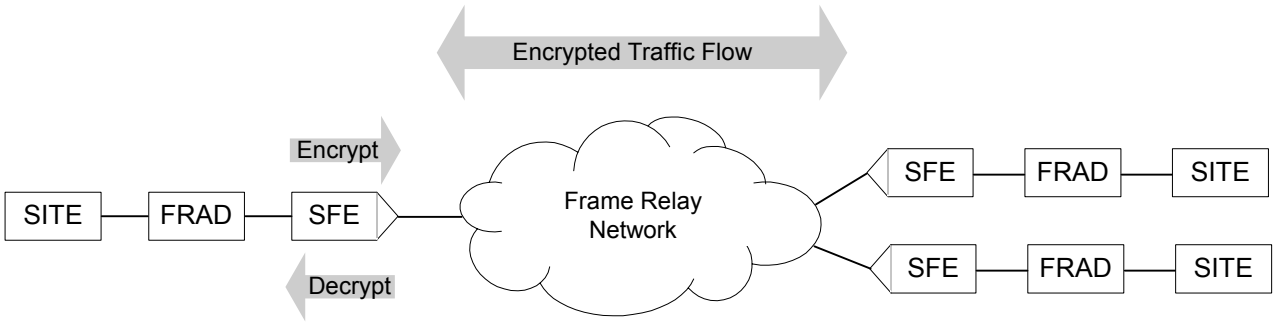
2 SafeEnterprise™ Frame Encryptor

2.1 Functional Overview

The SafeEnterprise™ Frame Encryptor (SFE) protects information flowing between nodes or sites of a frame relay network. The SFE can be configured to either allow or disallow information flow between two frame relay nodes. Furthermore, the information flow can be either protected through encryption or passed without encryption.

The role of the SFE is illustrated in Figure 1. The SFE is installed between a FRAD (Frame Relay Access Device) and a Frame Relay Network. A SFE dynamically configures with other SFEs in the network and builds secured connections between itself and the SFEs. The SFEs selectively encrypt, reject, or pass in the clear frames flowing from the FRAD to the network. Conversely the SFEs selectively decrypt, reject, or pass information flowing from the network to the FRADs.

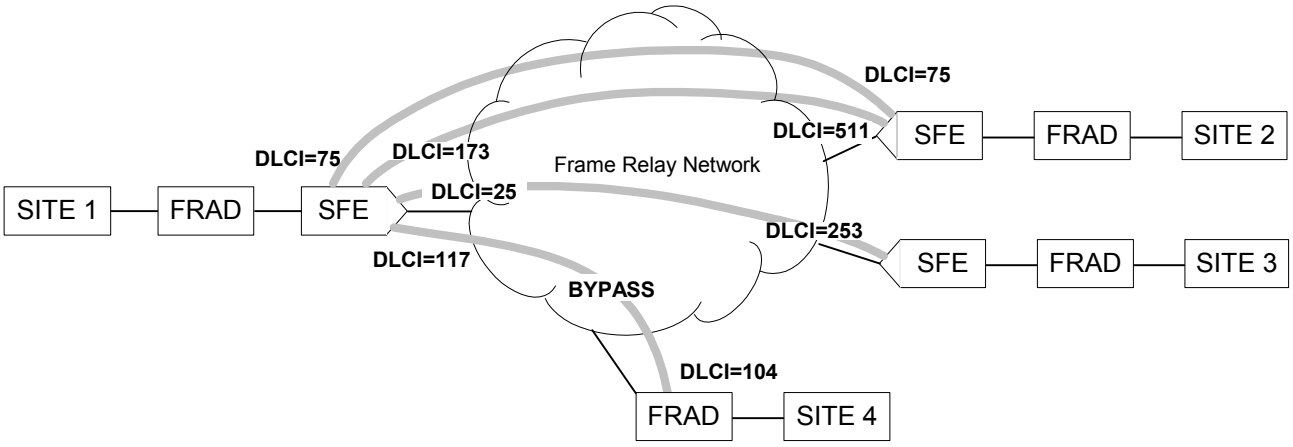
Figure 1. SFE Operation.



Secured connections are automatically established between the cryptographic module and similar units using a Diffie-Hellman key agreement process. This results in a separate secure link per connection and does not require any secret connection keys to ever be displayed or manually transported/installed. Secret connection keys never leave the secure boundary in clear text form and they are not stored in non-volatile memory in clear text form.

Figure 2 shows an example of three secured connections and one unsecured connection between sites. A secured connection is based on the DLCI (Data Link Connection Identifier), so it is possible to have more than one secured connection between two secure units. Since the frame relay network can change the value of the DLCIs, the DLCIs at each end of a secure connection usually have different values. In the example below there are 3 secured connections: 75-75, 173-511, and 25-253. Connection 117-104 is unsecured because a FRAD (frame relay access device) cannot handle encrypted traffic. This connection uses FIPS bypass mode to transfer data as plaintext.

Figure 2. SFE Usage Example.



The SFE can support a maximum of 1024 simultaneous connections. There are actually 976 connections available to the user at a frame relay network interface conforming to the Frame Relay Forum agreements; 48 more are reserved for user/net management.

2.2 Module Description

The SFE is a multiple-chip standalone cryptographic module comprised of production-grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 3. The encryptor provides data privacy and access control services for frame relay networks and supports up to 992 simultaneous crypto sessions. The frame encryptor can be deployed on X.21, V.35, and HSSI access links. There are three FIPS 140-2 validated models of the SafeEnterprise™ Frame Encryptor running the 5.00 firmware release:

- SFE Low Speed (SE-SFE-LixAC)
- SFE High Speed (SE-SFE-HixAC)
- SFE HSSI (SE-SFE-VVxAC)

The ‘i’ in the model numbers represents the interface kit; where ‘i’ may be:

- 2 X.21
- 3 V.35

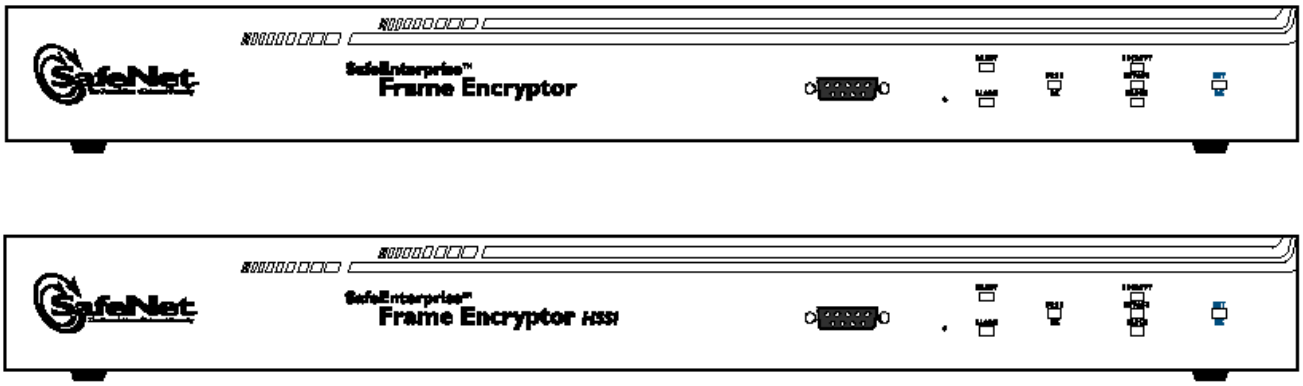
The ‘x’ in the model numbers represents the variants; where ‘x’ may be:

- A US power cord
- B UK power cord
- D Australian power cord
- E European power cord

2.2.1 Enclosure Indicators Connectors and Controls

All models share a common enclosure. The following figures present the front view, which is the same for all the models except for the labeling.

Figure 3. Frame Encryptor Front View.



SFE 027

The Frame Encryptor has two network interfaces located in the back of the module: the CLEAR interface connects to a physically secure private network and the CIPHER interface connects to an unsecure public network. While the rear view is similar for the three models, it is interface specific as illustrated in the follow figures.

Figure 4. Frame Encryptor (Low / High Speed) Rear View

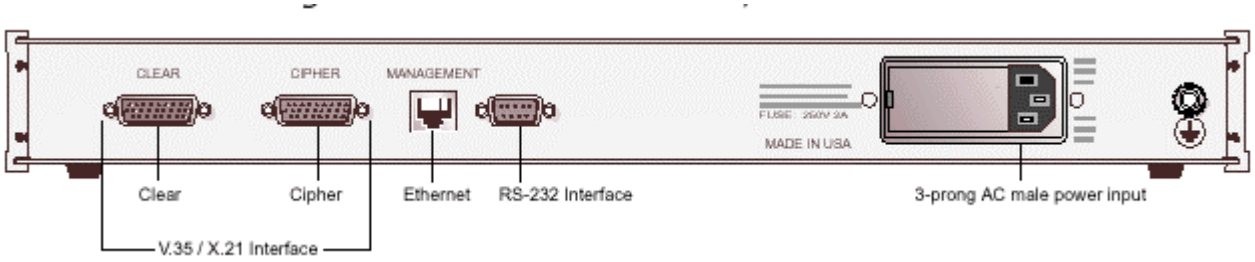
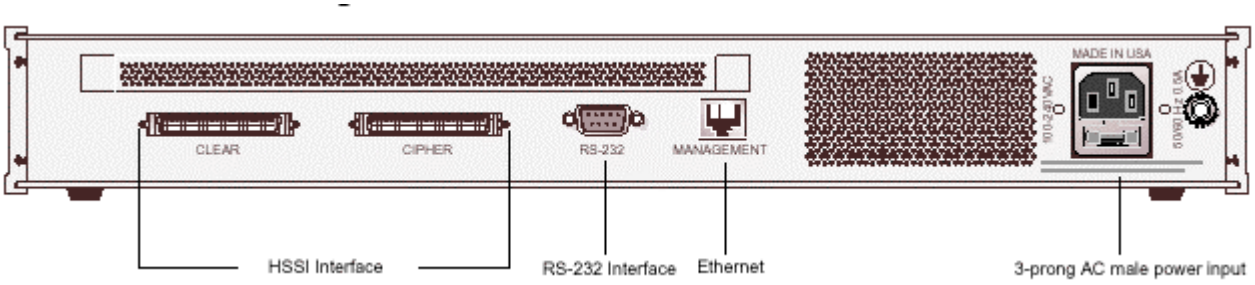


Figure 5. Frame Encryptor (HSSI) Rear View



Note: The SFE HSSI includes ventilation and internal fans for cooling.

2.3 Module Ports and Interfaces

The SafeEnterprise™ Frame Encryptor has five physical ports and four logical interfaces. The data input and output ports are located at the rear of the module. These ports are specific to the encryptor's network interface. The control interface is accessible on the RS-232 port on the front panel for limited operations such as system initialization. After system initialization is complete, an out-of-band control interface is provided on the Ethernet port located at the rear of the module and an in-band control interface is provided by the network interface. The

rear panel RS-232 port is reserved for future use and is disabled during normal operation. The front panel also contains LEDs for status output.

The **Data Input** and **Data Output** interfaces are constrained to the two data ports. All user data input and output is limited to the data ports as follows:

CLEAR Port:

- Connects to the user network, sending and receiving plaintext.

CIPHER Port:

- Connects to the external network, sending and receiving ciphertext.
- Sends authentication data, Diffie-Hellman public key components and ciphertext, to the far end module.
- Receives authentication data, Diffie-Hellman public key components and ciphertext, from the far end module.
- The SFE can be set to bypass, to send and receive plaintext for selected DLCI connections.

Control Input is provided by the front panel serial port, the Ethernet port and the CLEAR and CIPHER ports as follows:

- Front Panel RS-232 Serial port (used only for initialization prior to authentication and operation in the approved mode). It receives control input (protected via a username and password) from a local terminal.
- Ethernet port receives out-of-band control input (protected via a generated TDES key) from the SMC application.
- CLEAR and CIPHER ports may receive in-band control input (protected via a generated TDES key) from the SMC application.

Status output is provided by the front panel LEDs, the Front Panel RS-232 port, the Ethernet Port (out-of-band status), and the CLEAR and CIPHER ports (in-band status).

- Front panel LEDs indicate Ready, Alarm, Bypass Frame, Encrypted Frame, Blocked (Discarded) frame, and whether a frame is sent to the CIPHER or CLEAR port.
- The Front Panel RS-232 port returns status to a console.
- The Ethernet port may send out-of-band status output to the SMC application.
- The CLEAR and CIPHER ports may send in-band status output to the SMC application.

Electrical power is provided via the power supply connector at the rear of the unit.

2.4 Security Functions

The encryptor implements the following security functions:

Table 3. Module Security Functions.

Approved Security Function	*Certificate*
Symmetric Key Encryption	
AES **CFB128 (e/d; 128,192)**	32
TDES **TCFB64 (e/d; KO 1,2,3)** **TCFB-P64 (e/d; KO 1,2,3)**	139
TDES (Cylink Crypto Toolkit) **CFB8 (e/d; KO 1,2,3)**	22
SHS / DSS	
SHA-1 byte-oriented hashing and DSA	5
Random Number Generation	
DRNG (Compliant with FIPS PUB 186-2 Appendix 3.1)	N/A
Non-Approved Security Function	
Key Agreement	
Diffie-Hellman	N/A

The Frame Encryptor provides symmetric key encryption for data transferred through the module. The other security functions are utilized only for key negotiation and authentication of management access.

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

2.5 Approved Mode of Operation

When in the FIPS approved mode of operation, traffic received from the private network is encrypted before being transmitted out to the public network. Similarly, traffic received from the public network is decrypted before being transmitted out to the private network.

The encryptor must be configured to operate in **FIPS Mode using the SafeEnterprise Security Management Center (SMC).**.

Each SFE must have a unique Network Certificate (NC) issued under a common SMC. During the Diffie-Hellman key agreement, the SFEs mutually authenticate one another by exchanging Network Certificates in digitally signed messages. The SFE cannot build a secure connection with a remote SFE that does not have a valid Network Certificate. This mode of operation requires Security Management Center to issue the Network Certificates. In this mode, the SFEs protect against “replay attacks” by demanding a fresh challenge value for each signed Diffie-Hellman key agreement.

When a secure connection is established, a pair of SFEs share an encryption (session) key. When operating in this state, the two ends of the connection are in cryptographic synchronization using the TDES or AES algorithm. The SFE encrypts all data received from the CLEAR port (private network) and decrypts all data received from the CIPHER port (public network).

2.5.1 Bypass Mode

While the SFE is operating in the approved mode, one or more DCLI connections may be in bypass mode wherein data is passed as plaintext on the Data output port. Bypass mode is set when a far end cannot perform encryption or the connection has been explicitly set to pass plaintext data. Even on a connection that normally passes encrypted traffic, it is possible for some network management traffic to be passed as plaintext such as commands being passed to a switching router that resides in the frame relay network**.** The cryptographic module status output indicates whenever data is being passed as plaintext.

The module design prevents a single point failure from causing the module to pass plaintext data through the module on a secure connection. For the module to pass data in the clear, two independent internal actions are required. The policies, which allow plaintext data to be passed through the module, are established by two separate Crypto Officer configuration services and are implemented by two separate processes within the CM.

3 Security Policy Specification

3.1 Identification and Authentication

The SafeEnterprise™ Frame Encryptor employs identity-based authentication of operators. Operators using the console authenticate with a username and a password. Operators using SMC authenticate with SMC with a username and a password. The SMC application, in turn, authenticates with the SFE using certificates that are generated and signed by the SMC and stored within the cryptographic module. Operators 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.

The module supports one Crypto Officer role and four User roles. The Crypto Officer role provides full privileges for mode control, device configuration, and test functions. The User role services depend on the type of user as defined in Table 4.

Access to the authorized roles is restricted as follows:

Table 4. Roles and Required Identification and Authentication.

Role	*Type of Authentication*	*Authentication Data*
Network User	Identity-based	Network Users must present a certificate issued by the SMC.
Console Full User	Identity-based	Console Full Users must present a username and password.
Console Read-Only User	Identity-based	Console Read-Only Users must present a username and password.
Maintenance User	Identity-based	Console Maintenance Users must present a username and password.
Crypto Officer	Identity-based	Management (Ethernet) port access or in-band management (network port) access: - The operator is granted access to the Crypto Officer role after entering an appropriate username and password to access SMC.

Physical Maintenance is performed at the factory, as there are no services that require the cover to be removed in the field; although factory default settings may be restored in the field. The module should be zeriozed by a Crypto Officer before the module is returned to the factory, either by command or by removing the cover.

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

Table 5. Strength of Authentication.

Authentication Mechanism	Strength of Mechanism
Password	Users accessing the CM through the management 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 characters. The password must contain at least one uppercase character, one lowercase character, one numeric character (digit), and one special character. The possibility of correctly guessing a password is less than 1 in 1,000,000.
Network User Certificates	Network users must authenticate using 1024-bit DSS authentication. The possibility of deriving a private DSS key is less than 1 in 1,000,000
Certificate Exchange from SMC	Prior to initiating a certificate exchange the Crypto Officer must authenticate with SMC 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 characters. The password must contain at least one uppercase character, one lowercase character, one numeric character (digit), and one special character. The possibility of correctly guessing a password is less than 1 in 1,000,000.

3.2 Access Control

The SafeEnterprise™ Frame Encryptor access control policy specifies all services that are authorized for each role, and the type of access to Cryptographic Keys and CSPs available in each service.

The Crypto Officer role provides cryptographic initialization and management functions. Crypto Officer functions are available using SMC.

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 SFEs.)

The Console Full User can change some configuration settings.

Console Read-Only User is restricted to viewing status and alarms.

The Maintenance Role tampers the unit as soon as the role is activated. Then the maintenance role can restore manufacturing defaults or run the self-test.

3.2.1 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) employed within the SafeEnterprise™ Frame Encryptor.

Table 6. Cryptographic Keys and CSPs.

Data Item	Description
SFE Manufacturing Certificate	The X.509v3 certificate that identifies the SFE. It is produced and signed by the SafeNet Certification Authority (SCA). The certificate is signed/equipped with DSA keys.
SMC Manufacturing Certificate	The X.509v3 certificate that identifies the managing SMC system. It is produced and signed by the SafeNet Certification Authority (SCA). The certificate is signed/equipped with DSA keys.
Near End Network Certificate	The X.509v3 certificate that is associated with the SFE in an operational environment. It is produced and signed by the managing

Data Item	Description
	SMC system. The certificate is signed/equipped with DSA keys.
Far End Network Certificate	The X.509v3 certificate that is associated with the far end SFE in an operational environment. It is produced and signed by the managing SMC system. In Managed mode (the Approved mode of operation), this certificate is verified when it is received from the far end system, during operational mode changes. The certificate is signed/equipped with DSA keys.
Password	The operator password (and username) is used to access limited cryptographic module initialization functions via the console port. Operators are instructed to change the password during module initialization.
PRNG Initialization Vector	Defines the initialization point for the internal Pseudo Random Number Generator. It is initially set in the factory and its value is updated through the use of the PRNG.
PRNG Running Seed Key (XKEY)	Seed value for the internal Pseudo Random Number Generator.
Master Key	A TDES key that encrypts and decrypts keys and CSPs that are stored in the protected area of non-volatile RAM.
SFE DSS Private Key (X)	The secret component of the SFE DSS Key. (The public component of this key resides in the Near End Network Certificate.) This is a DSA key.
SMC/SFE (SNMP) Encryption Key	This is a TDES encryption key securing communications between the device and the management application.
Diffie-Hellman Private Key	This ephemeral key is used (along with the far-end SFE Diffie-Hellman public key) to agree on a session SFE/SFE encryption key.
Diffie-Hellman Public Key	This ephemeral key is sent to the far-end SFE for use in agreeing on a session SFE/SFE encryption key.
SFE/SFE Encryption Key	This is a TDES or AES encryption key securing communications between the mated SFEs.
SMC/SFE Message Counter Value	Counter maintained to mitigate message replay attacks between SMC and the SFE.

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

3.2.2 Services

The SafeEnterprise™ Frame Encryptor supports the services listed in the following tables. Each table describes the authorized services by the given operator role and identifies the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

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.)

Table 7. Console Full User – Roles and Services.

Authorized Services	*Cryptographic Keys and CSPs*	*Access Type*
Authenticate to the module.	Password	E
Change password	Password	W
Tamper – This service allows the operator to cause the unit to respond as though it has been physically tampered. This will result in: An active zeroization of the master secret key rendering other keys and CSPs stored in NVSRAM undecipherable. A software reset upon the cryptographic module This action will require the full tamper recovery process.	Master Key	W
Reset Unit – This service allows the user to reset (power-cycle) the CM. This action runs the power on self test.	Master Key DSA keys Diffie-Hellman Keys SFE/SFE key PRNG Init. Vector	E E W, E W, E E, W
Set Time – This service allows the operator to set the system clock.	None	N/A
Display Alarms – This service allows the operator to scroll through and view the contents of the CMs alarm queue.	None	N/A
Clear Alarm Condition – This service allows the operator to acknowledge an alarm condition. This will turn off the unit's Alarm LED.	None	N/A
Set Line Interface Parameters – This service allows the operator to configure the Line Interface. Items such as which clock source/type to use can be set.	None	N/A
Network Management: Display/set Cryptographic Module IP Address: This service allows the operator to display or set the value of the current IP address to which the Cryptographic Module will respond. Display/set connection (DLCI, etc.) to operate in loop back (for troubleshooting) Disable loop-back on connection (DLCI, etc.)	None	N/A
Display System Information – This service allows the operator to display the following information: Software Revision Hardware List Serial Number	None	N/A
Display Network Statistics – This service allows the operator to display network statistics for each port and connection.	None	N/A

Authorized Services	Cryptographic Keys and CSPs	Access Type
Display Cryptographic Connections – This service allows the operator to display: The state of each connection (DLCI, etc.) Traffic statistics of each connection (DLCI, etc.)	None	N/A

Table 8. Console Read-Only User – Roles and Services.

Authorized Services	Cryptographic Keys and CSPs	Access Type
Authenticate to the module.	Password	E
Display Alarms – This service allows the operator to scroll through and view the contents of the CMs alarm queue.	None	N/A
Network Management Display Cryptographic Module IP Address: This service allows the operator to display the current IP address to which the Cryptographic Module will respond. Display connection (DLCI, etc.) to operate in loop back (for troubleshooting).	None	N/A
Display System Information – This service allows the operator to display the following information: Software Revision Hardware List Serial Number	None	N/A
Display Network Statistics – This service allows the operator to display network statistics for each port and connection.	None	N/A
Display Cryptographic Connections – This service allows the operator to display: The state of each connection (DLCI, etc.) Traffic statistics of each connection (DLCI, etc.)	None	N/A

Table 9. Network User – Roles and Services.

Authorized Services	Cryptographic Keys and CSPs	Access Type
Authenticate to the module.	DSA Keys Diffie-Hellman Keys SFE/SFE Enc. Key	R, E W, E W
Encrypt – Encrypts data arriving on the CM's clear port and transmits it out the CM's cipher port. Encryption and decryption between two SFEs is transparent to human users. These users never have direct access to the encryption key.	SFE/SFE Encryption Key	E

Authorized Services	Cryptographic Keys and CSPs	Access Type
Decrypt – Decrypts data arriving on the CM's cipher port and transmits it out the CM's clear port. Encryption and decryption between two SFEs is transparent to human users. These users never have direct access to the encryption key.	SFE/SFE Encryption Key	E
Block data – Blocks data arriving on both the CM's cipher and clear ports.	None	N/A
Pass data – Passes data arriving on both the CM's cipher and clear ports.	None	N/A

Table 10. Crypto Officer – Roles and Services.

Authorized Services	Cryptographic Keys and CSPs	Access Type
Authenticate to the module.	DSA Private Key	E
Load a Network Certificate into the Cryptographic Module.	Near End Network Certificate	W, E
Establish an SMC/SFE connection encryption key.	SMC/SFE Encryption Key	W, E
Establish Console User Passwords – This service allows the operator to establish one or more console username and their associated passwords. Each username is configured to authorize the username to assume one or more console roles.	Master Key Password	E W
Set Operating Mode – This service allows the crypto officer to select the current operational mode. The crypto officer is permitted to command the Cryptographic Module into the following modes: Offline Operational Locked	None	N/A
Show Status – Output the current status of the Cryptographic Module: Active roles Cryptographic state of module. Cryptographic Module is in error state, error code If bypass capability exists, whether the bypass capability is enabled (on all channels / connections).	None	N/A
Set Default Configuration – This service allows the operator to force parameters settings back to their pre-configured default values.	None	N/A

Authorized Services	Cryptographic Keys and CSPs	Access Type
Set Cryptographic Parameters – This service allows the crypto officer to: Set the Maximum Connection Rekey Time Set the Failed Connection Retry Interval Set the Connection Setup Timeout Interval	None	N/A
Define Security Policy Parameters – This service allows the operator to: Set (optional) rule to block all traffic on a given connection Set (optional) permission to bypass security measures for a connection Set the CM Offline-Policy Define Secure Group Policy Define Secure Group Membership	None	N/A
Select Encryption Algorithms – This service allows the operator to select the algorithms to be used for SFE to SFE encryption.	None	N/A
Set FIPS 140-2 Mode – This service allows the operator to select whether FIPS 140-2 mode is enabled or disabled.	None	N/A
Define Second Action Policies – This service allows the operator to specify the "second action" required when data is to be passed in the clear. There are a number of settings so that the operator can selectively allow the passing of data for different traffic types.	None	N/A
Configure Trap Destination Table – This service allows the operator to configure and display the CM's trap destination table.	None	N/A
Reset Unit – This service allows the operator to reset (power-cycle) the CM. This action runs the power-on self-test.	Master Key DSA keys Diffie-Hellman Keys SFE/SFE key PRNG Init. Vector	E E W, E W, E E, W
Clear NVRAM – This service allows the operator to clear any active connection information and reset the CM.	Diffie-Hellman Keys SFE/SFE key	W W

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

Table 11. Maintenance – Roles and Services.

Authorized Services	Cryptographic Keys and CSPs	Access Type
Authenticate to the module.	Password	E
Zeroize System Memories – This service allows the operator to clear the various system memories thereby zeroing current configuration setting and certificates.	Master Key, Password, DSA Private Key PRNG Init. Vector All Certificates	W W W W W

Authorized Services	Cryptographic Keys and CSPs	Access Type
Set Default Configuration – This service allows the operator to force the operational settings back to the manufacturing default values. Note: The password for the default account is reset to the factory default value. All other CSPs were already zeroized by the act of tampering the module.	Password	W

3.3 Physical Security

The SafeEnterprise™ Frame Encryptor employs the following physical security mechanisms:

The SFE is made of commercially available, production grade components; 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 serious visible damage to the module.

Access to the circuitry contained within the SFE 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 all plaintext cryptographic keys and unprotected critical security parameters. This capability is operational whether or not power is applied to the module.

Tamper evident tape is placed over the cover retention screw.

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 retention screws which triggers the Tamper Switch. If the module detects tampering it erases the cryptographic keys and unprotected critical security parameters automatically. The module then enters into an error state and remains in that state until it is re-initialized.

If the Tamper Switch is triggered while the module is powered on, Tamper Alarms are asserted immediately and the module enters an error state. If the Tamper Switch is triggered while the module is powered off, Tamper Alarms will be asserted immediately after the module is powered on and the unit will enter an error state. While in the error state, the module will display a tamper indication 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 SafeEnterprise™ Frame 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. If the unit is tampered, the Tamper/Alarm LED is lit and all traffic is blocked.

3.4 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. The following table summarizes the system self tests.

Table 13. Self Tests.

Self Test	*Description*
Mandatory power-up tests performed at power-up and on demand.	
Cryptographic Algorithm	Each cryptographic function (TDES, AES, SHA-1, DSS), performed by the encryptor, is tested using a "known answer" test to verify the operation of the function.
Software/Firmware	The binary image of the encryptor's firmware includes a 16-bit error detection code (EDC) that allows the encryptor to verify the integrity of the firmware. A CRC is calculated on the program memory image and compared against the expected value, which is also stored in program memory.
Critical functions tests are 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 will be 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. They are tested for consistency, at the time they are generated, by using the public key to verify a signature created using the private key and a message digest.
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 load is verified via the DSA digital signature noted earlier in this document.
Continuous RNG	This test is a "stuck at" test to check the RNG output data for failure to a constant value.
Statistical RNG Test	Tests include the monobit, poker, and runs tests.
Bypass Test	This test verifies the correct operation of the cryptographic service when a switch takes place between a bypass and a cryptographic service.

3.5 Mitigation of Other Attacks

The SafeEnterprise™ Frame Encryptor is designed to mitigate replay attacks. It also mitigates the timing cryptanalysis attack described by Paul Kocher in *Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks*, extended abstract (7 Dec 1995). See the following table for details.

Table 14: Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Replay Attacks Between Encryptors	Incorporated into the Crypto Module Communication Protocol (CMCP) is a randomly generated Challenge Value. If the Challenge Value calculations are equal for two key exchange messages, the encryptor fails the key exchange.	None
Replay Attacks on Management Interface	Each PDU, exchanged between the encryptor and SMC, contains a 4-byte counter value. The value is incremented for each transmission between the encryptor and SMC. For PDUs transmitted by SMC, the counter value is always even. PDUs transmitted by the encryptor always contain an odd counter value. To be valid, the counter value must be greater than or equal to the counter value expected by the entity receiving the PDU.	None
Timing Cryptanalsys of Diffie-Hellman	A new random exponent is generated for every key agreement. This mitigates the potential of the noted timing cryptanalysis attack.	

4 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.

5 Appendix A – Operator Guidance

Introduction

This document provides information for crypto officers using the SafeEnterprise Frame Encryptor (referred to in this document as SFE) to enable them to install, configure, and operate the product in FIPS mode.

This document covers the three SFE models: SFE Low Speed, SFE High Speed, and SFE-HSSI.

There are two pertinent user groups for the SFEs:

- **Crypto Officers –** One or more Crypto Officers will operate the Frame Encryptor performing administrative operations. The list of operations is defined in the Security Policy with details provided in the *SafeEnterprise™ Security Management Center User's Guide.*
- **Network Users –** Multiple human users may make use of the services of the Frame Encryptor to create, use and destroy data link connection identifiers (DLCIs). The human users do not access the module cryptographic services directly. Rather, the act of using the protected networks causes two or more encryptors to establish secure connections providing the services like key generation and encryption/decryption services by way of the frame encryptor protocols. The cryptographic module is essentially transparent to the human users.

Crypto officers are the only class of operators that can modify security-relevant settings on the cryptographic module. Therefore the guidance information in this document pertains only to crypto officers. This document does not provide guidance for users.

Crypto Officer Guidance

SFE administrators operate the SFE device (referred to in this document as the *module*) in the FIPS role of crypto officer.

> **IMPORTANT: Read all of the instructions in this document before installing, configuring, and operating the Frame Encryptor Gateway.**

Frame Encryptor Delivery

On receiving the SFE module, perform the following steps:

1. Inspect the device for signs of tampering. Check that the tamper evident tape and the covers of the module do not show any signs of tampering. If tampering is detected, return the device to the manufacturer.
2. Inspect the label on the bottom of the SFE to ensure you have the correct FIPS approved version of the hardware which will be one of the following:
   - SFE Low Speed: P/N: 14976-120-04
   - SFE High Speed: P/N: 14976-110-04
   - SFE HSSI: P/N: 16673-010-02

If the module shows signs of tampering or has an incorrect label, do not install the product. Contact your organization's security officer for instructions on how to proceed.

If the module does not show signs of tampering and has the proper label, proceed to the next section.

Frame Encryptor Initial Configuration

Initial configuration instructions are provided mainly in the *SafeEnterprise™ Frame Encryptor User's Guide*.

Be sure to use the settings and steps provided in this section to constrain the initial configuration actions as described in the *SafeEnterprise™ Frame Encryptor User's Guide* so that the Frame Encryptor module is not compromised during the configuration phase. This approach ensures the module boots properly and enters FIPS 140-2 approved mode.

Then return to this document for special instructions to finish configuring the device to operate in FIPS mode.

1. When starting up the SFE for the first time, use the console port for performing initial configuration operations.
2. Log in using the default username and password.
3. The lower portion of the screen provides a system summary. Ensure that the Software Version information includes: **XXXXX-0500-XX**.

   This indicates that the firmware version is 5.0. If the version number is other than **0500**, return the module to the manufacturer. If the version is correct, proceed with the configuration.
4. Change the default password. The new password must be a minimum of 8 characters using a combination of upper and lower case letters, numerals and punctuation (any typable characters including spaces but not tab characters or return characters). Select:
   - **Administration (IP Address)**
   - **Change Password**
   - **Change Password**
   - Follow the prompts to complete the operation.
5. Set the device IP address. The IP address must be consistent with the addressing of the operational network. Select:
   - **Administration (IP Address)**
   - **Change Device IP Parameters**
   - **Enter New IP Parameters**
   - Follow the prompts to complete the operation.

When you have changed the password and set the IP address, you can complete configuration tasks using the instructions in *SFE Installation and Configuration*. Then continue on to final configuration using the SafeEnterprise Security Management Center (SMC).

Frame Encryptor Final Configuration

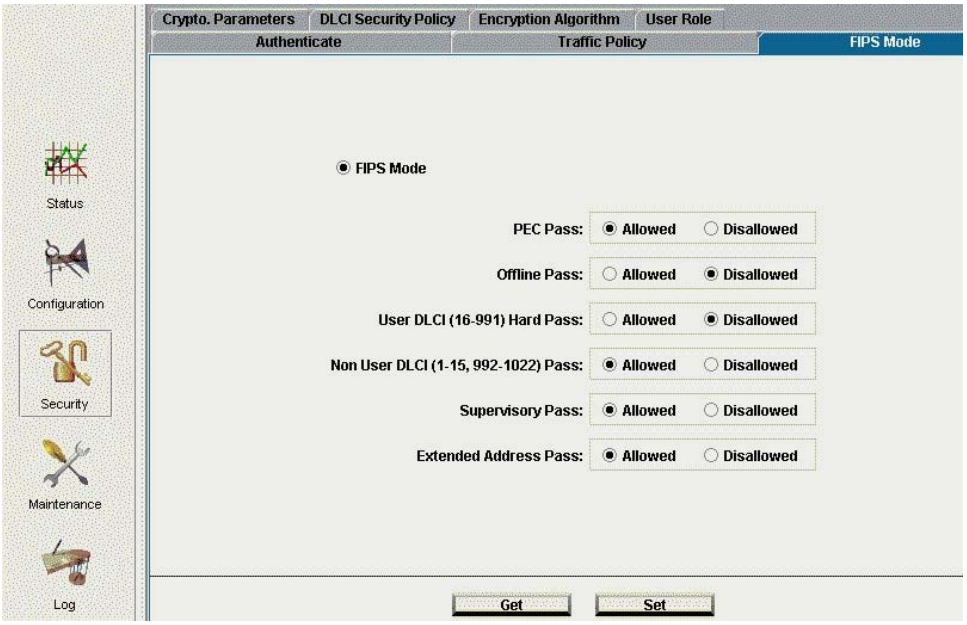
When using the SafeEnterprise Security Management Center (SMC) to finish configuring the SFE, follow these steps to ensure the module operates in a FIPS-approved manner. User the *SafeEnterprise™ Security Management Center User's Guide* as needed for reference.

1. Authenticate the SFE to SMC as described in the *SafeEnterprise™ Security Management Center User's Guide*. Use the Manufacturing Certificate from the floppy diskette that shipped with the SFE.
2. Select the device's Encryption Algorithms.

   Note: While included in the list of Encryption Algorithms, Cylink (SafeNet) Encapsulation has to do with the mechanism used to encapsulate the Frame Relay traffic. It may need to be selected for correct operation in the network. Regardless, when operating in FIPS Mode, the SFE enforces the use of only the FIPS approved algorithms for all security operations.
3. Use the Traffic Policy tab to assign the Traffic Handling policies for the SFE.
4. Use the DLCI Security Policy tab to assign the DLCI Security policies for the SFE.
5. Use the FIPS Mode tab to set FIPS Mode and the FIPS redundant security settings. The following settings are recommended to prevent passing of plain text data over channels that are normally encrypted:

PEC Pass	Allowed or Disallowed
Offline Pass	Disallowed
User DLCI 16-991 (Hard Pass)	Disallowed
User DLCI 1-15, 992-10-22 Pass	Allowed or Disallowed
Supervisory Pass	Allowed or Disallowed
Extended Address Pass	Allowed or Disallowed

6. Select FIPS Mode by clicking the FIPS Mode radio button.



At any time you can view this screen to confirm the module is operating in the FIPS Approved mode of operation. In this mode, only FIPS approved cryptographic algorithms and security functions are performed.

To run the self-test at any time, recycle the power. This briefly interrupts services, but original connections will be restored when the unit powers up again.

7. Establish the Secure Group association(s) for the SFE. (This operation is completed from the Security Menu in the main SMC window.)
8. Finally, set the SFE to the **Operational** or **Locked** configuration to bring it online and establish secure connections.