SafeNet
The Foundation of Internet Security

SafeEnterprise™ Link Encryptor

The Foundation of Internet Security

Security Policy

SafeEnterprise™ Link Encryptor
FIPS 140-2 - Level 2 Validation
Non-Proprietary Security Policy
(14885-5 revision 1.0)

Classic Hardware Models

NRZ-H	(SE-SLE-HNxAC)
NRZ-L	(SE-SLE-LNxAC)
T1	(SE-SLE-1ExAB)
E1 75 Ohm	(SE-SLE-27xAB)
E1 120 Ohm	(SE-SLE-2ExAB)
RS-232	(SE-SLE-LRxAB)

HSSI & T3 Hardware Models

HSSI	(SE-SLE-VVxAB)
T3	(SE-SLE-37xAB)

with

4.01 Firmware

1 Introduction

This document is the Security Policy for the SafeEnterprise™ Link 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 2. 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 Link 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 (CMV) Program 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™ Link Encryptor can be found at http://safenet-inc.com.

In this document, the SafeEnterprise™ Link Encryptor is also referred to as “the module”, “the encryptor”, “the Link Encryptor” and “SLE”.

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™ Link Encryptor meets the overall requirements applicable to Level 2 security for FIPS 140-2, with Physical Security and Design Assurance meeting the Level 3 requirements.

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

2 SafeEnterprise™ Link Encryptor

2.1 Module Description

The SafeEnterprise™ Link Encryptor 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 2. The encryptor provides data privacy and access control services for networks utilizing point-to-point technologies. The encryptors can be deployed on NRZ, EIA-232, T1, E1, T3 and HSSI access links. There are eight FIPS 140-2 certified models of the SafeEnterprise™ Link Encryptor running the 4.01 firmware release:

- HSSI (SE-SLE-VVxAB)
- T3 (SE-SLE-37xAB)
- NRZ-H (SE-SLE-HNxAC)
- NRZ-L (SE-SLE-LNxAC)
- T1 (SE-SLE-1ExAB)
- E1 75 Ohm (SE-SLE-27xAB)
- E1 120 Ohm (SE-SLE-2ExAB)
- RS-232 (SE-SLE-LRxAB)

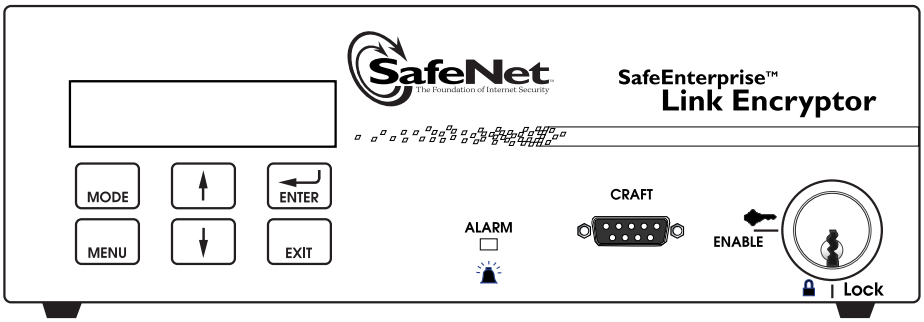
The ‘x’ in the model numbers represents the variants; where ‘x’ may be:

- A US power cord
- B UK power cord
- D Australian power cord
- E European power cord
- V -48V DC power

The models share two basic enclosures. The following figure presents the front view of the HSSI and T3 models.

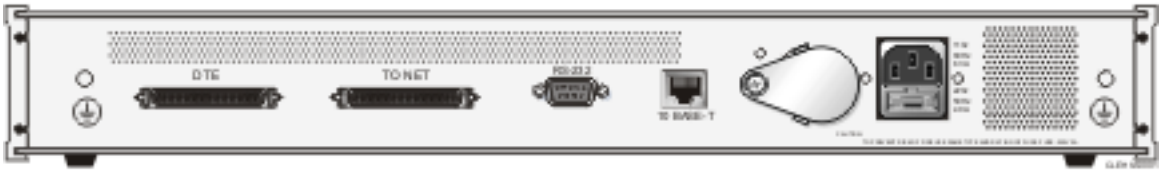
Link Encryptor HSSI and T3 Front View

The remainder of the models are considered “Link Classic” units and share the front view presented in the following figure.

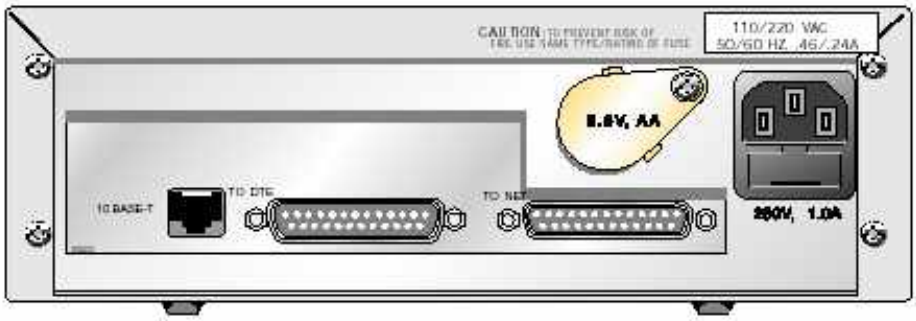


Link Encryptor Classic Front View

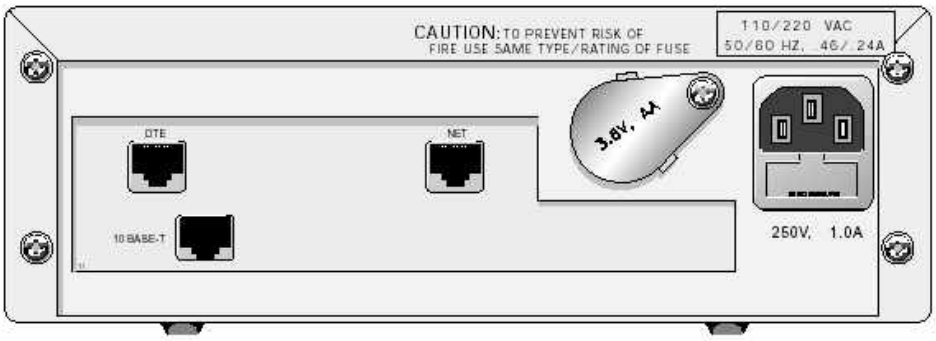
The Link Encryptor HSSI is the only model with an internal fan, the rest of the Link Encryptor models contain no moving parts. The encryptor has two network interfaces: one for attachment to a physically secure private network and the other for attachment to an unsecure public network, located in the back of the module. While the rear view is similar for the different models, it is interface specific as illustrated in the follow figures.



Link Encryptor (HSSI) Rear View



Link Encryptor (RS232) Rear View



Link Encryptor (T1) Rear View

2.2 Module Ports and Interfaces

The SafeEnterprise™ Link Encryptor has four 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 Ethernet port, for the control interface, is also located at the rear of the module, while a special serial port is located on the front panel. (The serial port provides a limited control interface for system initialization.) The front panel also contains the Medeco lock along with the keypad, LCD screen and Alarm LED for status output.

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

- DTE Port:
  - Connects to the user network.
  - Receives plaintext from the user network.
  - Sends plaintext to the user network.
- NET Port:
  - Connects to the external network.
  - 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.

Control Input is limited to the front panel keypad, Ethernet port and the serial port. (The serial port is used only for initialization prior to authentication and operation in the approved mode.)

Note: The Medeco lock acts as a selector for the control input interface. When in the enabled position, the front panel keypad is active and the Ethernet port is disabled; when in the locked position, the Ethernet port is enabled and the front panel keypad is disabled.

- Front panel keypad:
  - Allows input of configuration parameters when the Medeco lock is in the enabled position.
- Ethernet port:
  - Receives control input (protected via a generated TDES key) from the SMC application when the Medeco lock is in the locked position.
  - Sends status output (protected via a generated TDES key) to the SMC application.
  - Optionally sends non-security affecting status, in the form of SNMP traps, to other monitoring applications.

Status output is limited to the front panel LCD and LED

- Front panel LCD and LED:
  - Select module status is displayed on the LCD.
  - Internal alarm conditions light the Alarm LED.

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

2.3 Security Functions

The encryptor implements the following security functions:

Approved Security Function	*Certificate*
Symmetric Key Encryption	
AES • **CFB1 (e/d; 192)**	32
TDEA • **TCFB-P1 (e/d; KO 1,2,3)**	139
TDEA (Cylink Crypto Toolkit) • **CFB8 (e/d; KO 1,2,3)**	22
SHS / DSS	
SHA-1 byte-oriented hashing and DSA	5
Non-Approved Security Function	
Key Agreement	
Diffie-Hellman	

The Link 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 the connection only after the encryptor has positively identified and authenticated the remote encryptor.

2.4 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 the **Network Certified** authentication mode with the security mode set to **Secure** to be operating in the FIPS 140-2 approved mode.

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

Within the Authenticated Mode, Secure is the normal operating state. To enter Secure, a pair of SLEs must share an encryption (session) key. When operating in this state, the two ends of the transmission link are in cryptographic synchronization using the TDES or AES algorithm. The SLE encrypts all date received from the DTE (private network) and decrypts all data received from the public network.

To place the encryptor in the approved mode of operation, complete the following:

1. **Authenticate** the device via SMC.
2. Select the **Network Certified** Authentication Mode from SMC’s *Security/System Control* panel.
3. Select the **Secure** Operational Mode from SMC’s *Configuration/Operational Mode* panel.

3 Security Policy Specification

3.1 Identification and Authentication

The SafeEnterprise™ Link Encryptor employs role-based authentication of the operator. The module supports two roles: the User Role and the Crypto Officer Role. The User Role is restricted to viewing status and alarms, while the Crypto Officer role provides full privileges for mode control, device configuration, and test functions.

Access to the authorized roles, for operators, is restricted as follows:

Role	*Type of Authentication*	*Authentication Data*
User	Role-based	The User role is authenticated at SMC by a user id and password combination that grants viewing privileges. No changes, or updates, may be initiated by an operator in the User role. Similarly, some status information is presented on the front panel display, but the keypad is disabled to the User role.
Crypto Officer	Role-based	Front panel access - Possession of the Medeco key to unlock the device

Role	Type of Authentication	Authentication Data
		authenticates the operator as a Crypto Officer. Management (Ethernet) port access - The operator is granted access to the Crypto Officer role after entering an appropriate user id and password to access SMC.

Table 1: Roles and Required Identification and Authentication

An operator is authenticated to the Crypto Officer role at the front panel through possession of the key that will turn the Medeco lock to the Enable position. Concurrent operator access/operation is prevented by disallowing SNMP access (from SMC) when the Medeco lock is set to **enable** the front panel.

Physical Maintenance shall be performed at the factory, as there are no services that require the cover to be removed in the field. Similarly, there are no logical maintenance services performed 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:

Authentication Mechanism	Strength of Mechanism
Physical Medeco lock and key	Possession of the Medeco key.
Certificate Exchange from SMC	Prior to initiating a certificate exchange , the Crypto Officer must authenticate, with SMC, using a password that is at least 6 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 likelihood of correctly guessing a password is less than 1 in 1,000,000.

Table 2: Strengths of Authentication Mechanisms

3.2 Access Control

The SafeEnterprise™ Link 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 via the front panel keypad or SMC.

The User Role is restricted to viewing status and alarms.

3.2.1 Cryptographic Keys and CSPs

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

Data Item	Description
SLE Manufacturing Certificate	The X.509v3 certificate that identifies the SLE. It is produced and signed by the SafeNet Certification Authority (SCA).

Data Item	Description
	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 SLE in an operational environment. It is produced and signed by the managing 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 SLE 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.
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.
SLE DSS Private Key (X)	The secret component of the SLE DSS Key. This is a DSA key.
SMC/SLE (SNMP) Encryption Key	This is a TDES encryption key securing communications between the device and the management application.
SLE/SLE Encryption Key	This is a TDES or AES encryption key securing communications between the mated SLEs.
SMC/SLE Message Counter Value	Counter maintained to mitigate message replay attacks between SMC and the SLE.

Table 3: Cryptographic Keys and CSPs

Note: While the above table lists the certificates that may be on the encryptor, the certificates only contain public information.

3.2.2 Services

The SafeEnterprise™ Link Encryptor supports the services listed in the following table. The table groups the authorized services by the operator roles 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.)

Role	Authorized Services	Cryptographic Keys and CSPs	Access Type

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
User	Show Operational Mode / Status 1) View Trap Information 2) View Audit Log 3) View Communication Parameters 4) View Trap Forwarding Parameters 5) View Event Browser.	None	R
	Encrypt / Decrypt (Encryption and decryption, between two SLEs or between SMC and an SLE, is transparent to the user. The user never has direct access to the encryption key.)	SLE/SLE Encryption Key SMC/SLE Encryption Key	E
Crypto Officer	Set Operational Mode: Allows the operator to set the operational mode to Clear, Standby or Secure mode. *Note: Clear is not an approved Operational mode. If the encryptor is operated in a Clear mode, it is in a non-FIPS mode of operation.*	None	E
	Alarm/Event 1) Display Event Log: Allows the operator to scroll through and view the contents of the encryptor's event log. 2) Clear Event Log: This service allows the operator to completely clear the contents of the event log. 3) Display Exception Log: Allows the operator to scroll through and view the contents of the encryptor's exception log. 4) View Counts of Self-Test Pass vs. Self-Test Attempted	None	R, E
	Set Time/Date: Allows the operator to set the real time clock to the current date and time.	None	E

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
	Key Management 1) Set Auto Key Change Attributes 2) Days Interval 3) End to End Delay 4) Clear Modes Allowed/Disallowed 5) Mode NET CERT, MANUAL (authentication) KEY, UNAUTH DH 6) Adapt Algorithm Allowed/Disallowed 7) Select the "Blocking Pattern" used during key exchange, and in Standby mode *Note: As with the Clear mode noted earlier, the MANUAL KEY and UNAUTH DH Key Management Modes are not FIPS approved modes. NET CERT is the FIPS approved mode of operation.*		E
	Key Management 1) Zeroize Keys: Allows the operator to erase critical security parameters. When this service is activated the CSPs are actively erased.	Near End Network Certificate SLE DSS Private Key (X) SMC/SLE (SNMP) Encryption Key SMC/SLE SNMP Message Counter SLE/SLE Encryption Key PRNG Running Seed Key (XKEY)	E
	Network Management 1) Display/Set Unit IP Address 2) Display/Set Gateway IP Address 3) Display/Set Subnet Mask Address 4) Display/Set Trap1/Trap2 IP Address	None	R, E

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
	Line Interface Configuration (E1, T1) 1) Display/Set Framing 2) Display/Set Line Coding 3) Display/Set Equalization for Net and DTE interfaces Line Interface Configuration (NRZ-H, NRZ-L, RS232) 1) Display/Set Clock Source and Clock Inversion for Net and DTE interfaces 2) Display/Set control signal (CTS, RTS) actions 3) Display/Set Physical Interface Type 4) Display/Set Dial-up configuration a) Enabled/Disabled b) Link Up Signal c) Link "Drops to" Mode d) Secure "Fails to" Mode	None	R, E
	System Test: Allows the operator to set or clear the loopback configuration.	None	R
	Display Manufacturing Info: Allows the operator to display general information about the module.	None	R
	Set Default Configuration	None	E
	Firmware Update	SMC DSS Public Key	R, E
	Authenticate: Establish the authorized link between SMC and the encryptor.	SLE DSS Private Key (X) Near End Network Certificate SMC Manufacturing Certificate	E, W W

Table 4: Services Authorized for Roles

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

3.3 Physical Security

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

1. The SLE is made of commercially available, production grade components; all integrated circuit chips have passivation applied to them.

2. The SLE contains a tamper evident security label that provides visible evidence of any attempt to remove the cover from the chassis.

3. Access to the circuitry contained within the SLE is restricted by the use of tamper response and zeroization circuitry along with the Medeco lock. Attempting the removal of the cover, whether or not the lock has been unlocked, 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.

4. Access to the front panel keypad is restricted by the use of the Medeco lock. When in the locked position, the module disables the keypad to prevent unauthorized changes to the module parameters. When locked, it also provides a second barrier to the removal of the cover. Finally, the key cannot be removed from the lock when it in the enabled position.

Attempts to remove the module cover are considered tampering. Movement of the cover relative to the chassis greater than 0.0625 inch triggers the Tamper Switch.[1] If the encryptor detects tampering it erases the cryptographic keys and unprotected critical security parameters automatically. The encryptor 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 recommendations should be considered in the implementation of a Security Policy governing the installation and operation of the SafeEnterprise™ Link Encryptors:

1. Secure access to the Encryptor within a physically secure, limited access room or environment.

2. Once initialized and operational, store the module keys in a separate location.

The following table outlines the recommended inspection and/or testing of the physical security mechanisms.

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.	The security label should be in place and should not show any signs of an attempt to remove the cover from the chassis. The encryptor displays a tampered message on the front panel display when in the tampered state. In addition, all traffic is blocked.
Medeco Lock	Visual inspection in accordance with organization's Security Policy.	The lock should be in the locked position and the key should be stored in a separate, secured location.

Table 5: Inspection/Testing of Physical Security Mechanisms

[1] Physical access to cryptographically relevant components of the module requires the cover to be moved greater than 0.325 inches.

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.

Self Test	*Description*
Mandatory Power-up Tests	**Mandatory self tests which are 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	**The following additional self 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 shall attempt 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	**Self 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.

3.5 Mitigation of Other Attacks

The SafeEnterprise™ Link 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.

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.	
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.	
Timing Cryptanalsys of Diffie-Hellman	A new random exponent is generated for every key exchange. This mitigates the potential of the noted timing cryptanalysis attack.	

Table 6: Mitigation of Other Attacks

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.