Senetas Corporation Ltd.

CN1000 Fibre Channel Encryptor

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

October 2011

(Doc No.) v1.0.9

Table of Contents

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the Senetas Corporation Ltd. "CN1000 Fibre Channel Encryptor v1.9.3" cryptographic module. This Security Policy specifies the security rules under which the module operates to meet the FIPS 140-2 Level 3 requirements.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2), *Security Requirements for Cryptographic Modules*, specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive but unclassified information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the NIST/CSEC Cryptographic Module Validation Program (CMVP) and the FIPS 140-2 standard, visit www.nist.gov/cmvp .

This Security Policy, using the terminology contained in the FIPS 140-2 specification, describes how the CN1000 Fibre Channel Encryptor complies with the eleven sections of the standard. In this document, the CN1000 Fibre Channel Encryptor is also referred to as "the module" or "the encryptor".

This Security Policy contains only non-proprietary information. Any other documentation associated with FIPS 140-2 conformance testing and validation is proprietary and confidential to Senetas Corporation Ltd., and is releasable only under appropriate non-disclosure agreements. For more information describing the CN Series systems, visit http://www.senetas.com.

1.1 References

For more information on the FIPS 140-2 standard and validation program please refer to the National Institute of Standards and Technology website at www.nist.gov/cmvp.

The following standards from NIST are all available via the URL: www.nist.gov/cmvp .

- *FIPS PUB 140-2: Security Requirements for Cryptographic Modules.*
- *FIPS 140-2 Annex A: Approved Security Functions.*
- *FIPS 140-2 Annex B: Approved Protection Profiles.*
- *FIPS 140-2 Annex C: Approved Random Number Generators.*
- *FIPS 140-2 Annex D: Approved Key Establishment.*
- *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.*
- *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197.
- *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3.
- *DES Modes of Operation*, Federal Information Processing Standards Publication 81.
- *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2.
- *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-3.
- ATM Security Specification (Version 1.1), af-sec-0100.002, The ATM Forum Technical Committee, March, 2001.

1.2 Document History

Authors	Date	Version	Comment
Senetas Security	26-May-2009	1.0.0	First submission 1000 Series Security Policy.
Senetas Security	12-Jan-2010	1.0.1	Coordination review.
Senetas Security	28-Jan-2010	1.0.2	Coordination review 2nd Edition
Senetas Security	23-Mar-2011	1.0.3	Fibre Channel re-verification
Senetas Corporation Ltd	11-Jul-2011	1.0.4	Modified Security Policy document to be Fibre Channel specific
Senetas Corporation Ltd	14-Jul-2011	1.0.5	Review comments incorporated
Senetas Corporation Ltd	6-Sep-2011	1.0.6	Updated certificate numbers
Senetas Corporation Ltd	6-Sep-2011	1.0.7	Final edits pre submission
Senetas Corporation Ltd	30-Sep-2011	1.0.8	CSC QA review notes incorporated
Senetas Corporation Ltd	5-Sep-2011	1.0.9	CSC Final Review

1.3 Acronyms and Abbreviations

AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
CAT	Connection Action Table
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FC	Fibre Channel
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GFC	Generic Framing Protocol
HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
IV	Initialization Vector

KAT	Known Answer Test
LED	Light Emitting Diode
Mbps	Megabits per second
NC	Network Certificate
NIST	National Institute of Standards and Technology
NTU	Network Termination Unit
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comment
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SAN	Storage Area Network
SDH	Synchronous Digital Hierarchy
SFP	Small Form-factor Pluggable (transceiver)
SHA-n	Secure Hash Algorithm
SONET	Synchronous Optical Network
VCAT	Virtual Channel Action Table
X.509	Digital Certificate Standard RFC 2459

1.4 Definitions

The following Senetas product designators have been updated from those referenced by FIPS140-2 Cryptographic module validation certificate 1267.

New designators

CN1000	New identifier for CypherNET 1000 platform
CN3000	New identifier for CypherNET 3000 platform
CN Series	Refers to the CN1000 and CN3000 encryptor family

Legacy designators

CypherNET	Legacy designator for the CN Series encryptors
CypherNet	Legacy designator for the CN Series encryptors

2. Product Description

The CN1000 Fibre Channel Encryptor is a multiple-chip standalone cryptographic module consisting of production-grade components contained, in accordance with FIPS 140-2 Level 3, in a physically protected enclosure. Excluding the pluggable interface (SFP) transceivers, the module's outer casing defines the cryptographic boundary. The encryptor is completely enclosed in a steel case which is protected from tampering by internal tamper protection circuitry and external tamper response seals. Any attempt to remove the cover automatically erases all sensitive information stored internally in the cryptographic module.

The module meets the overall requirements applicable to Level 3 security for FIPS 140-2.

Table 1 Module Compliance Table

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

2.1 Module Identification

The CN1000 Fibre Channel Encryptor v.1.9.3 provides data privacy and access control services for Fibre Channel networks. See model details summarized in Table 2. Data privacy is provided by FIPS approved AES and Triple-DES algorithms. The complete list of approved module algorithms is included in the *Approved Security Function* table.

Table 2 CN1000 Fibre Channel Model

Model	Interface / Protocol (Cryptographic Module)	Notes
A5175B	4 Gbps – Fibre Channel This model supports pluggable transceivers which are considered to be outside the cryptographic boundary. (2088 Module)	AC power

2.2 Operational Overview

2.2.1 General

The CN1000 Fibre Channel (FC) encryptor operates in a point-to-point network topology. Encryptors are typically installed between an operators' private network equipment and public network infrastructure. Securing an optic fibre link that connects two remote office sites is a common installation application. Figure 1. provides a operational overview of two CN1000 encryptors positioned in the network.

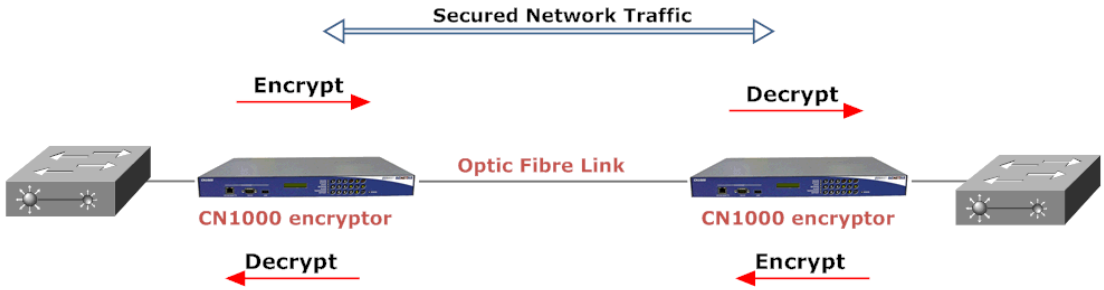


Figure 1 - Operational Overview

The data path between two encryptors is referred to as a `connection`. The term `session` refers to a connection that has been securely established and is processing data according to a defined encryption policy. The Connection Action Table (CAT) stores the processing rules for each policy.

The CN1000 Fibre Channel encryptor supports policy options of 'Secure` and 'Discard` and these apply to all data carried on each connection.

The default policy for a pair of connected encryptors is `Discard`. In this mode user data is not transmitted to the public network.

In order to enter `Secure` mode and pass information securely, each encryptor must be `Certified` by the same trusted body and exchange a secret `Session Key` using the RSA key exchange process (as specified in the ATM Forum's ATM Security Specification version 1.1). If the session key exchange is successful this results in a separate secure session per connection, without the need for secret session keys to be displayed or manually transported and installed.

Figure 2. (overleaf) illustrates the conceptual data flow through a CN1000 encryptor.

1. Information arrives at the encryptor's interface ports
2. The encryptor looks up a connection rule in the Connection Action Table (CAT) which specifies how that information is to be processed,
3. The information is processed according to the rule and (if not being discarded) is encrypted and sent out the opposite port

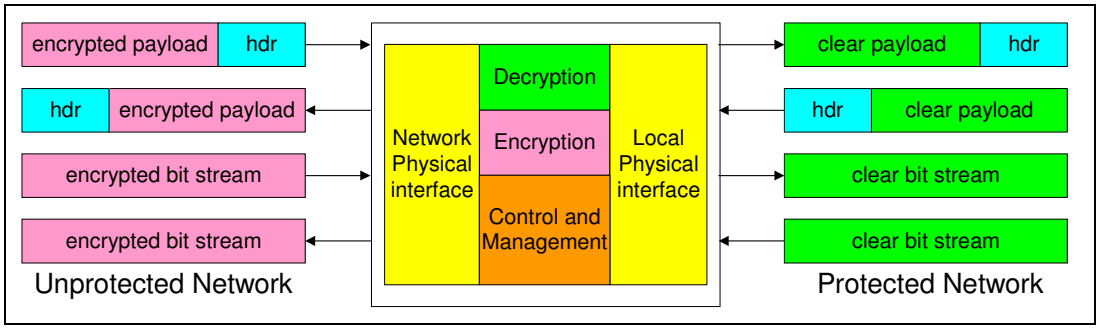


Figure 2 - Data Flow Through the Encryptor

2.2.2 Encryptor management

Encryptors can be centrally controlled or managed across local and remote stations using Senetas' `CypherManager` Remote Management application. Encryptors support both *in-band* and *out-of-band* SNMPv3 management. *In-band* management interleaves management messages with user data on the encryptor's network interface port whilst *out-of-band* management uses the dedicated front panel Ethernet port. A Command Line Interface (CLI) is also available via the console RS-232 port.

2.2.3 Fibre Channel implementation

Fibre Channel is the de-facto interconnection technology for storage networking and is optimised for the efficient movement of data between server and storage systems in a Storage Area Network (SAN).

Acting as a `Bump in the Fibre`, the CN1000 can secure point-to-point Fibre Channel network connections operating at speeds up to 4.25Gbps. Figure 3. shows a typical Fibre Channel installation in which the encryptors are deployed on a public network link. In this example the encryptors provide a secure connection between two SAN components; a File Server and remote Disk Array.

Fibre Channel information is sent in discrete frames as per the Fibre Channel ANSI standard (ANSI INCITS 424-2007). The standard defines a multi-layer hierarchy of which the CN1000 Fibre Channel encryptor implements FC-0, FC-1 and the required FC-2 layer functionality to enable network interoperability with Direct Fibre, Fibre with Repeater, GFP-T and GFP-F connections. In order to interwork with Fibre Channel network devices the FC-2 header is only partially encrypted. The *Source identifier*, *Destination identifier* and *Frame Type* fields of the frame header are left unencrypted. The remaining header fields and payload are encrypted.

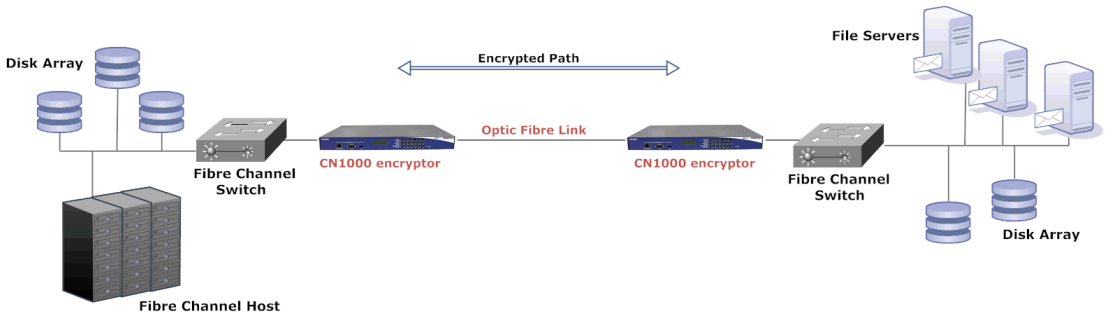


Figure 3 – Fibre Channel Configuration

3. Module Ports and Interfaces

3.1 CN1000 Ports

The encryptor user access ports, LCD display and Keypad are located on the front of the module as presented in Figure 4.

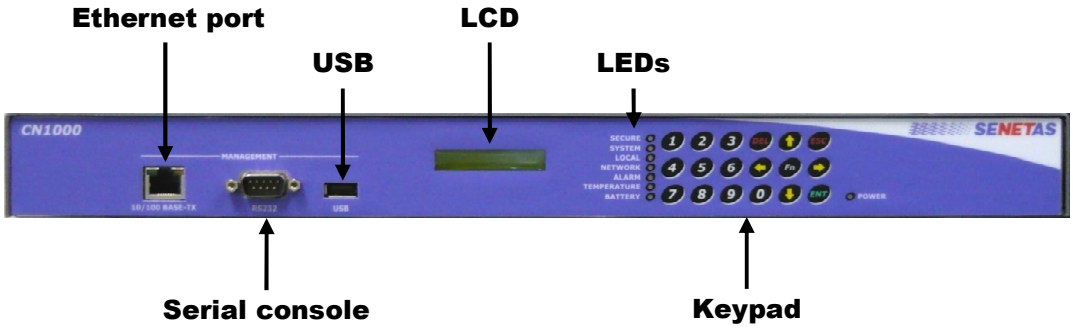


Figure 4 - Front View of CN1000

The encryptor has two data interface ports (Local and Network) located in the rear of the module as presented in Figure 5.

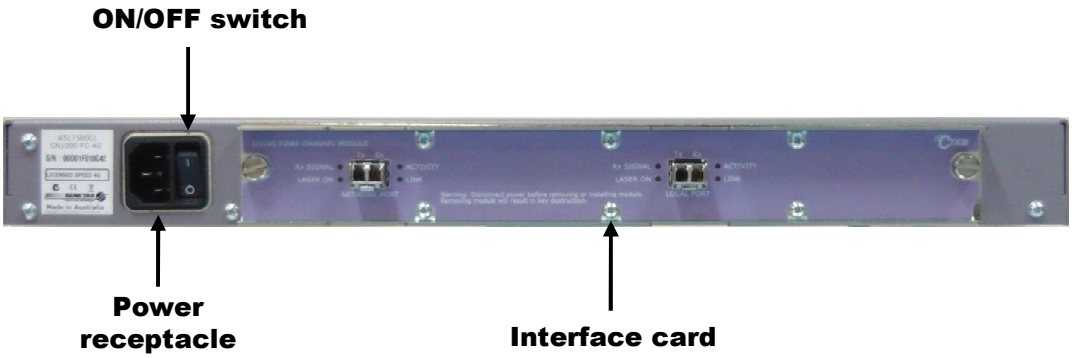


Figure 5 - Rear View of CN1000

The Local Port connects to the physically secure private network while the Network Port connects to an unsecured public network.

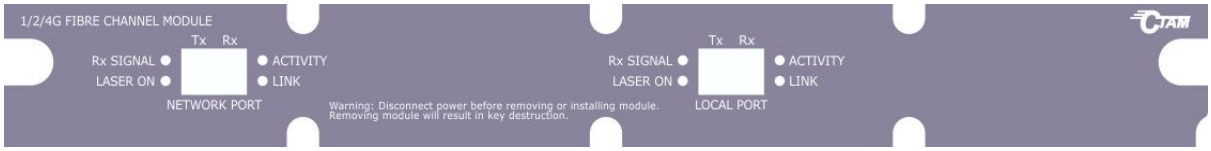


Figure 6 - A5175B 1/2/4 Gbps (SFP) Fibre Channel dual port label

The rear panel also contains a tamper evident seal that indicates movement of the module interface card with respect to the module enclosure. See Section 5, Physical Security for details.

Table 3 defines the Physical Ports.

Table 3 Physical Ports

Port	Location	Purpose
RJ-45 Ethernet	Front Panel	Allows secure and authenticated remote management by the CypherManager application.
DB9 RS-232 Serial Console	Front Panel	The Serial Console port connects to a local terminal and provides a simple command line interface for initialization prior to authentication and operation in the approved mode. This port also allows administrative access and monitoring of operations. User name and password authentication is required to access this port.
USB	Front Panel	The USB port provides the Crypto Officer with a mechanism for applying approved and properly signed firmware updates to the module.
Keypad	Front Panel	Allows entry of initialization commands.
LCD	Front Panel	Displays configuration information in response to commands entered via the keypad. Also indicates the state of RSA keys and certificates.
LEDs	Front Panel	Indicate the system state, including alarms.
LEDs	Rear Panel	Indicate network traffic.
Network Port	Rear Panel	The Network Port connects to the public network; access is protected by RSA certificates. The Network Port is of the same interface type as the Local Port.
Local Port	Rear Panel	The Local Port connects to the private network; access is protected by RSA certificates. The Local Port is of the same interface type as the Network Port.
Power Connector	Rear Panel	Provides power to the module.

3.2 CN1000 Encryptor Interfaces

Table 4 summarizes the FIPS 140-2 defined Logical Interfaces.

Table 4 Logical Interfaces

Interface	Explanation
Data Input	Interface through which data is input to the module.
Data Output	Interface by which data is output from the module.
Control Input	Interface through which commands are input to configure or control the operation of the module.
Status Output	Interface by which status information is output from the module.

The FIPS 140-2 Logical Interfaces map to the Physical Ports as outlined in Table 5.

Table 5 FIPS 140-2 Logical Interface to Physical Port Mapping

FIPS 140-2 Logical Interface	CN1000 Interface	Physical Port
Data Input	Private Network Interface	Local Port
	Public Network Interface	Network Port
Data Output	Private Network Interface	Local Port
	Public Network Interface	Network Port
Control Input	Local Console	DB9 RS-232 Serial Console
	Keypad & Display	Keypad / LCD
	CypherManager Remote Management Interface	Management RJ-45 Ethernet Port
	Private Network Interface	Local Port
	Public Network Interface	Network Port
Status Output	Local Console	DB9 RS-232 Serial Console
	Keypad & Display	Keypad / LCD
	CypherManager Remote Management Interface	Management RJ-45 Ethernet Port
	Private Network Interface	Local Port
	Public Network Interface	Network Port
	LEDs	Front & Rear LEDs
Power	Power Switch	Power Connector

The Fibre Channel Encryptor supports the FIPS 140-2 Logical Interfaces as outlined in Table 6.

Table 6 Interface Support

Logical Interface	Support
Data Input & Data Output	**Local Interface:** • Connects to the local (private) network; sends and receives plaintext user data to and from the local network. **Network Interface:** • Connects to the public network; sends and receives ciphertext user data, via the public network, to and from a far end cryptographic module. • Authenticates with the far end cryptographic module(s); sends and receives authentication data and RSA key exchange components to and from a far end module. The module can be set to bypass allowing it to send and receive plaintext user data for selected connections.
Control Input	Control Input is provided by the Local Console, Keypad & Display, and CypherManager Remote Management Interface as follows: • The Keypad supports module initialization prior to authentication

Logical Interface	Support
	and operation in the approved mode. A Crypto Officer sets the IP address for remote administration by CypherManager; sets the system clock; and loads, in conjunction with CypherManager, the module's certificate. • As an alternative to using the Keypad, the Local Console may be used for initialization prior to certification and operation in the approved mode. The Local Console receives control input from a locally connected terminal. • Following initialization and authentication, the CypherManager application can communicate with the module to receive out-of-band control input. When configured for in-band management, the Private and Public Network Interfaces may also receive control input. In this mode, the CypherManager application sends control input by way of the Local or Network Port rather than the RJ-45 Ethernet.
Status Output	Status output is provided by the Keypad & Display, LEDs, Local Console and CypherManager Remote Management Interface as follows • The Display presents the Crypto Officer with the command data being entered via the Keypad. It also indicates the state of the RSA keys and certificates. • The LEDs indicate error states, state of the local and network interfaces, alarm, temperature, battery state and network traffic. • As an alternative to using the Keypad & Display, the Local Console may be used for initialization prior to certification and operation in the approved mode. The Local Console may also be used for monitoring some operations; status output is sent to a locally connected terminal. • Following initialization and authentication, the module sends out-of-band status output to the CypherManager application. When configured for in-band management, the Private and Public Network Interfaces may also send status output. In this mode, the module status output is sent to the CypherManager application by way of the Local or Network Port rather than the RJ-45 Ethernet Port.

The encryptor does permit logically distinct categories of information to share the Local and Network Ports. If the module is configured to allow in-band management traffic, then the control/status information (key exchange or management commands) and user data enter and exit the module via the Network Interfaces. The module separates these two logically distinct categories of information, using the mechanisms specific to the operational protocols.

- Fibre Channel systems use the SOFi4 unused ordered set in conjunction with a proprietary header type for key management and for segregating in-band management traffic.

4. Roles, Services and Authentication

The cryptographic module supports four roles: Crypto Officer, Operator, Upgrader and User. Crypto Officers are assigned permissions based on one of two subcategories: Administrator and Supervisor. The supported roles are summarized in Table 7.

Table 7 Roles

Role	Description
Crypto Officer	**Administrator:** Provides cryptographic initialization and management functions. Crypto Officer functions are available via CypherManager. Limited functions are also available via the Console interface.
	Supervisor: Provides limited operational management functions. Functions are available via CypherManager. Limited functions are also available via the Console interface.
	Services for the CO are accessible directly via the Local Console CLI or remotely via the CypherManager Remote Management Interface and the CypherManager application.
User	Restricted to read-only access to module configuration data.
	Operator: Services for the Operator are accessible directly via the Local Console CLI or remotely via the CypherManager Remote Management Interface and the CypherManager application.
	Upgrader: The Upgrader Role is limited to applying field upgrades to the module firmware. Additional access is restricted to read-only access to module configuration data.
	Services for the Upgrader are accessible directly via the Local Console CLI or remotely via the CypherManager Remote Management Interface and the CypherManager application.
	The **User** Role is available in conjunction with other authenticated modules. The User Role negotiates encryption/decryption keys and uses encryption/decryption services.
	User services are only indirectly accessible based on the connections configured with other cryptographic modules.

Roles cannot be changed while authenticated to the module; however, the module permits multiple concurrent operators. While only one operator may connect to the Local Console at a time, multiple concurrent remote sessions are permitted. CypherManager based management is not session oriented; thus, multiple operators may be issuing commands with each command processed individually as it is received by the module. In a meshed network the system architecture supports simultaneous interactions with many far end modules; the multiple users (remote modules) all sending data to the data input port. The module's access control rules, system timing, and internal controls maintain separation of the multiple concurrent COs, Operators, Upgraders and Users.

The module does not support a maintenance role. Since there are no field services requiring removal of the cover, physical maintenance is performed at the factory.

> Note: A Crypto Officer should zeroize the module before it is returned to the factory. The module can be zeroized by command or by removing the network interface card(s).

4.1 Identification and Authentication

The module employs Identity-Based Authentication. Access is restricted as indicated in Table 8. Up to 30 unique names and passwords may be defined for operators (COs, Operators, Upgraders) of the module. Operators using the Local Console enter their name and password to authenticate directly with the module. Operators using CypherManager issue commands to the encryptor. Password based authentication and Diffie-Hellman Key Agreement allow the transport of secure messages to the module. Commands from CypherManager are individually authenticated to ensure Data Origin Authentication and Data Integrity. Data Origin Authentication, based on the names and passwords, ensures the authenticity of the user claiming to have sent the command. Users employing the module's security functions and cryptographic algorithms, over the Data Input and Output ports, authenticate via certificates that have been generated and signed by a common CypherManager. The Users exchange master and session keys using RSA public key wrapping.

Table 8 Authentication Type

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based	Crypto Officers using the Local Console present unique user names and passwords to log in to the CLI. Crypto Officers using CypherManager have unique identities embedded in the command protocol. Each issued command is individually authenticated.
Operator	Identity-based	Operators follow the same authentication rules as Crypto Officers.
Upgrader	Identity-based	Upgraders follow the same authentication rules as Crypto Officers.
User	Identity-based	Users (remote encryptors) authenticate to each other with their CypherManager issued certificates.

The strength of the authentication mechanisms is detailed in Table 9.

Table 9 Strength of Authentication

Authentication Mechanism	Strength
Password	COs, Operators, and Upgraders accessing the module CLI, via the Local Console, must authenticate using a password that is at least 8 characters and at most 16 characters in length. 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 14.5 million) possible combinations. The possibility of correctly guessing a password is less than 1 in 1,000,000. After three failed authentication attempts via the CLI, the Local Console port access is locked for 3 minutes. With the 3 minute lockout, the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. Note: The module also suppresses feedback of authentication data, being entered into the Local Console, by returning blank characters.
User Certificates	Far end modules (Users) authenticate using an RSA authentication certificate based on a 1024, 2048 or 4096 bit keys. The possibility of deriving a private RSA key is less than

Authentication Mechanism	Strength
	1 in 1,000,000. Based on the multi-step handshaking process between modules, the possibility of randomly guessing the passphrase in 60 seconds is less than 1 in 100,000.

4.2 Roles and Services

The CN1000 Fibre Channel Encryptor supports the services listed in the following tables. The tables group the authorized services by the module's defined roles and identify 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)

D - The item is **deleted** by the service.

The module's services are described in more detail in the CN Series documentation.

The following basic services are Unauthenticated . They either require physical access to the module or are used in establishing the operator's authorized role. With the exception of power cycling (to run the Self Tests) or physically tampering the module, all Crypto Officer services require the operator to be Authenticated. For a Crypto Officer, the process of authenticating establishes the access level (Administrator, Supervisor or Operator) afforded to the operator. Power cycling or physically tampering the module requires physical access to the CN1000 Fibre Channel Encryptor.

Table 10 Unauthenticated Services

Service	Cryptographic Keys and CSPs	Access Type
Run Self Test (Power Cycle the Module)	Initialization Vector	D,W
	RSA Public Key	D,W
	RSA Private Key	D,W,E
Authenticate operator [1]	Password (HMAC-SHA-1)	R,E
	Console: Plain Password	R,E
Tamper	System Master Key	W

[1] Once authenticated, the module establishes whether the operator is authorized for CO (Administrator, Supervisor), Operator or Upgrader access.

Once authenticated, the operator has access to the services required to initialize, configure and monitor the module. With the exception of passwords associated with user accounts, the operator never enters Cryptographic Keys or CSPs directly into the module (an Administrator CO will enter passwords when working with user accounts).

Table 11 Operator – Roles and Services

Crypto Officer		User			Authorized Service	Cryptographic Keys and CSPs	Access Type
Admin	Supv	Oper	Upgr	User			
✓	✓				Set Real Time Clock	none	W
✓					Load Module Certificate	RSA Public and Private Keys	W
						RSA Public Key Certificate	W
✓					Create User Account	Password	W
✓					Modify User Account	Password	E, W
✓					Delete User Account	Password	D
✓	✓	✓	✓		View User Account	none	R
✓	✓				Edit Connection Action Table (Bypass)	none	W
✓	✓	✓	✓		View Connection Action Table	none	R
✓	✓	✓	✓		Show Firmware Version	none	R
✓					Clear Audit Trail	Password	W
✓	✓	✓	✓		View Audit Trail	none	R
✓					Clear Event Log	Password	W
✓	✓	✓	✓		View Event Log	none	R
✓	✓	✓	✓		View FIPS Mode Status	none	R
✓	✓				Change FIPS Mode Status	Password	W
✓	✓				Run Self Test (Reboot Command)	Password	E
✓			✓		Install Firmware Update	none	E
✓[1]	✓[1]				Generate Session Key	AES or Triple-DES Session Keys	W
✓[1]	✓[1]				Generate Initialization Vector	Initialization Vector	W
✓[1]	✓[1]				RSA signature generation	RSA Private Key	R, E

Crypto Officer		User			Authorized Service	Cryptographic Keys and CSPs	Access Type
Admin	Supv	Oper	Upgr	User			
✓[1]	✓[1]				RSA signature verification	RSA Public Key	R, E
✓					Erase Module – Zeroize (Console Command)	System Master Key and all CSP data stored in non-volatile memory	W
✓[2]	✓[2]			✓[2]	Establish a Remote Session	Privacy Key	R, W, E

[1] Restarting a connection causes new session keys to be generated.
[2] Privacy keys are established when a remote session is initiated and used to encrypt and decrypt all subsequent directives.

Note: Plaintext Cryptographic Keys and CSPs are never output from the module regardless of the operative role or the mode of operation.

5. Physical Security

The CN1000 Fibre Channel Encryptor employs the following physical security mechanisms:

1. The encryptor is made of commercially available, production grade components meeting commercial specifications for power, temperature, reliability, shock and vibration. All Integrated Circuit (IC) chips have passivation applied to them. The steel enclosure is opaque to the visible spectrum. The ventilation holes on the encryptor's sides are factory fitted with baffles to obscure visual access and to prevent undetected physical probing inside the enclosure. Attempts to enter the module without removing the cover will cause visible damage to the module, while removing the cover will trigger the tamper circuitry.
2. Access to the internal circuitry is restricted by the use of tamper detection and response circuitry which is operational whether or not power is applied to the module. Attempting to remove the enclosure's cover causes the immediate zeroization of the System Master Key (a 168-bit symmetric key which is used to encrypt the unit's private key and user localized passwords). Zeroization of the System Master Key renders all cryptographic keys and CSPs indecipherable.
3. Two tamper evident seals are pre-installed (at factory). The first is placed over the interface module face plate, between the interface card and the underside of the main enclosure. The second is placed between the top cover and underside of the main enclosure (refer Figure 7). Attempting to remove the interface card or top cover to obtain access to the internal components of the module will irreparably disturb these seals, thus providing visible evidence of the tamper attempt. Note that it is not physically possible to remove the enclosure lid without first removing the interface card.

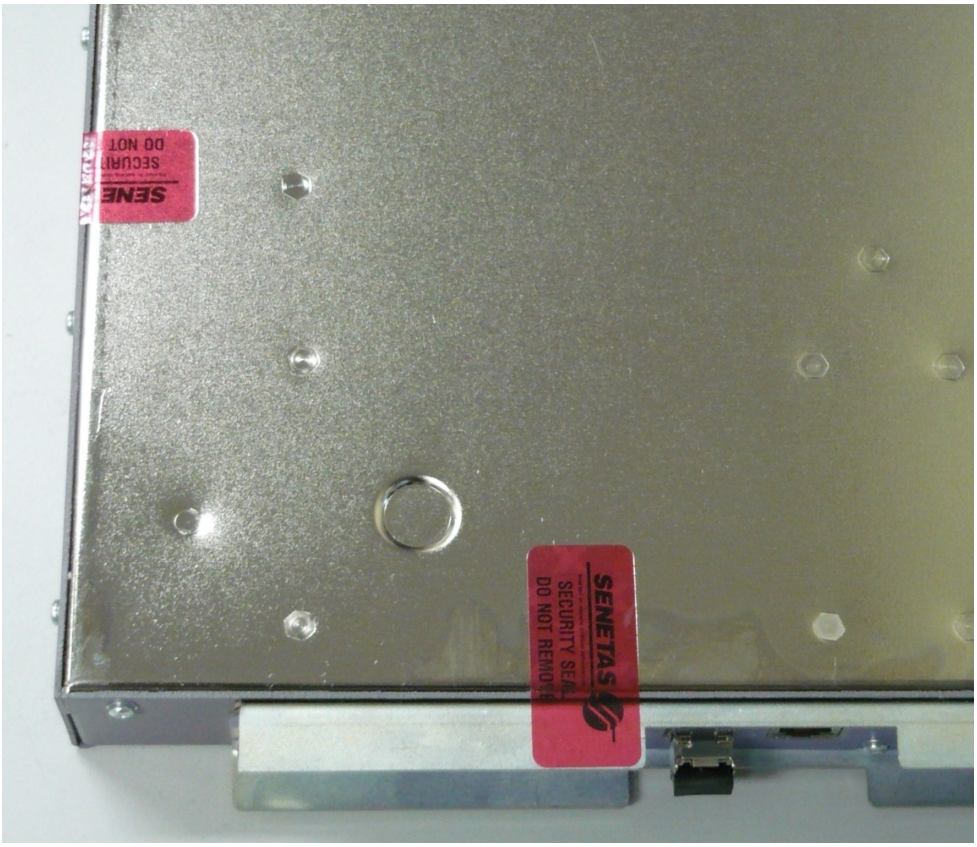


Figure 7 – Factory installed tamper seals

Access to the cryptographically relevant components of the module requires the cover to be removed, and any attempt to remove the module cover is considered tampering. Removal of the cover requires removal of the network interface card(s) which triggers the Tamper Circuit. Should the tamper circuit be triggered, the module zeroizes the System Master Key. All data previously encrypted by the System Master Key is no longer able to be decrypted correctly, including cryptographic keys and CSP data. The module then returns to an uncertified state and remains in that state until it is checked and re-certified. The Tamper Circuit is active at all times; the specific tamper response differs slightly based on the module's power state.

1. The module is powered on when the Tamper Circuit is triggered:
   The module zeroizes the System Master Key. It also erases any active key material and logs an event message indicating that the network interface card has been removed. After tamper activation, the system is uncertified and the Secure LED (on the front panel) is illuminated red until the module is re-certified (a new certificate is loaded). Whilst in the uncertified state, CLI and CypherManager access are active, but no user data is output.
2. The module is powered off when the Tamper Circuit is triggered:
   The module zeroizes the System Master Key. Since the module does not retain active key material across power cycles, there is no additional key material to be zeroized. The event message is logged and the Secure LED (on the front panel) is illuminated red after the module is once again powered on. When the Tamper Circuit is triggered, the module powers on to the uncertified state. Whilst in this state, CLI and CypherManager access are active, but no user data is output.

While the physical security mechanisms protect the integrity of the module and its keys and CSPs, it is strongly recommend that the cryptographic module be maintained within a physically secure, limited access room or environment.

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

Table 12 Physical Security Inspection & Test

Security Mechanism	Inspection & Test Guidance	Frequency
Tamper Evidence	Tamper indication is available to all user roles via the alarm mechanism and evidence by the physical tamper labels. The Crypto Officer is responsible for the physical security inspection. During normal operation, the Secure LED is illuminated **green**. When the unit is uncertified (has no loaded certificate as either the default factory manufactured state or user erase operation has been executed) or in the tampered state, the Secure LED is illuminated **red** and all traffic is blocked. Inspect the enclosure and tamper evident seals for physical signs of tampering or attempted access to the cryptographic module.	In accordance with organization's Security Policy.
Tamper Circuit	The module enters the tampered state when the circuit is triggered. Once in this state, the module blocks all user traffic until the module is physically reset.	No direct inspection or test is required; triggering the circuit will block all data flow.

6. Cryptographic Key Management

6.1 Cryptographic Keys and CSPs

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

Table 13 Cryptographic Keys and CSPs

Key	Use	Storage
System Master Key	On initialization, the module generates a 168-bit symmetric key. This key encrypts, using 3-key Triple-DES CFB8, the module's public and private RSA keys and the user table stored in the configuration flash memory.	Stored, as plaintext, in a tamper protected memory device. On tamper, the System Master Key is zeroized rendering the encrypted data, in the configuration flash memory, undecipherable.
RSA Private Key	This 1024 or 2048 bit key is the secret component of the module's RSA Key pair. It is generated when the module receives a Load Certificate command from CypherManager. The RSA Private Key is used to authenticate connections with other encryptors and to unwrap master session keys and session keys received from far-end encryptors.	Stored, in 3-key Triple-DES-encrypted format, in non-volatile memory. On tamper, the Triple-DES System Master Key is zeroized, rendering the encrypted RSA Private Key undecipherable.
RSA Public Key	This 1024 or 2048 bit key is the public component of the module's RSA Key pair. It resides in the Network Certificate, and is used for authenticating connections with other encryptors.	Stored, in 3-key Triple-DES-encrypted format, in Flash Memory. On tamper, the Triple-DES System Master Key is zeroized, rendering the encrypted RSA Public Key undecipherable.
Module Certificate	The X.509v3 certificate is associated with the module in an operational environment. It is produced and signed by the managing CypherManager system to establish root trust between encryptors. Once the certificate has been authenticated, Far-end encryptors use the embedded RSA Public Key to wrap the initial session keys used to encrypt a session. Alteration of the certificate will result in an authentication failure between encryptors.	Stored, in the clear, in non-volatile system memory. The certificate is deleted from memory only on an Erase command from a Crypto Officer.
Authentication Password	Up to 30 unique Crypto Officers (Administrator, Supervisor or Operator) may be defined, with associated passwords, within the module. The CLI uses the Authentication Password to authenticate Crypto Officers accessing the system via the Local Console. CypherManager requires an operator password that is used to uniquely authenticate each command to the	Passwords and their associated Usernames are hashed and stored in the User Table which is stored 3-key Triple-DES-encrypted format in non-volatile memory. On tamper, the Triple-DES System Master Key is zeroized, rendering the

Key	Use	Storage
	module.	encrypted Passwords undecipherable.
Session Master Key	For each session, the module generates a symmetric session master key using the ANSI X9.31 PRNG. The seed key and seed value are not part of the stored CSP data, but are generated on demand as required. RSA key exchange is used to transfer this key to a far-end encryptor. The session master key persists for the life of the session and is used to secure the active session keys that may be changed periodically during the session.	All session keys are held in volatile system memory and destroyed at the end of a session.
Session Keys	For each session, the module also generates two session keys for each data flow path in the secure connection (one for the Initiator-Responder path and another for the Responder-Initiator path) using the ANSI X9.31 PRNG. These keys Triple-DES or AES encrypt and decrypt the user data transferred between the encryptors. These active session keys are normally changed periodically based on the duration of the session.	All session keys are held in volatile system memory and destroyed at the end of a session.
Privacy Keys	For each remote management session, the module generates an AES privacy key using Diffie-Hellman to secure the control / flow path in the secure connection. The key is generated using the ANSI X9.31 PRNG.	All privacy keys are held in volatile system memory and destroyed at the end of a remote management session.
X9.31 PRNG Seed Key	For each ANSI X9.31 PRNG operation, the RNG Seed Key is sourced from the hardware RNG device.	The ANSI X9.31 Seed key is held in volatile system memory and destroyed on power cycle.
X9.31 PRNG Seed	For each ANSI X9.31 PRNG operation, the RNG Seed is sourced from the hardware RNG device.	The ANSI X9.31 Seed is held in volatile system memory and destroyed on power cycle.

Note: While the certificates, maintained within the module, are listed as CSPs, they contain only public information.

The module prevents data output during system initialization. No data is output until the module is successfully authenticated and the module certificate has been properly loaded. Following system initialization, the module prevents data output during the self tests associated with a power cycle or reboot event. No data is output until all self tests have completed successfully. The module also prevents data output during and after zeroization of cryptographic keys and CSPs; zeroization occurs when the tamper circuit is triggered. In addition, the system's internal modules and timing controls work together to isolate the CSP and key management functions from the user data input and output processes.

6.2 Cryptographic Algorithms

The CN1000 Fibre Channel Encryptor employs the following approved cryptographic algorithms.

Table 14 FIPS Approved Algorithms

Algorithm Type	Algorithm	FIPS Validation Certificate	Target Model
CN Series Crypto Library			**CN1000**
Symmetric Key	**Triple-DES** TCBC (e/d; KO 1) TCFB8 (e/d; KO 1,2) TCFB64 (e/d; KO 1,2)	TDES # 1158	
	AES CBC (e/d; 128,256) CFB128 (e/d; 128,256)	AES # 1786	
Asymmetric Key	**RSA** ALG[ANSIX9.31]; Key(gen) (MOD: 1024, 2048, 4096; PubKey Values: 65537) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 1024, 2048, 4096, SHS: SHA-1, SHA-256, SHA-512	RSA # 893	
	DSA KEYGEN(Y) MOD(1024) SIG(gen) MOD(1024) SIG(ver) MOD(1024)	DSA # 562	
Hashing	SHA-1 (BYTE only) SHA-256 (BYTE only) SHA-512 (BYTE only)	SHS # 1568	
HMAC	HMAC-SHA-1 (Key Sizes Ranges Tested: KS<BS) HMAC-SHA-256 (Key Sizes Ranges Tested: KS<BS) HMAC-SHA-512 (Key Sizes Ranges Tested: KS<BS)	HMAC # 1051	
RNG	ANSI X9.31	RNG # 948	

CN1000 2088 Module			**Fibre Channel Model** 1/2/4 Gbps subassembly for A5175B – 4 Gbps FC
Symmetric Key	**AES** CFB128 (e/d; 256)	AES # 1775	

In addition to the FIPS approved algorithms, the CN1000 Fibre Channel Encryptor module also includes the following algorithms.

Table 15 Non-FIPS Algorithms

Function	Use
RSA Key Wrapping	Per the ATM Forum Security Specification (Version 1.1), RSA key wrapping is employed to establish the symmetric keys used for data encryption between cryptographic modules.
Diffie-Hellman Key Agreement	Diffie-Hellman Key Agreement is employed to establish the symmetric keys used to secure the management interface between CypherManager and the cryptographic module.
Non-deterministic RNG	A non-deterministic hardware RNG device is used to source seed and seed key to the X9.31 PRNG operation.
MD5	Non approved hashing function.

Note: 1024 or 2048 bit keys, providing the equivalent of 80 or 112 bits of symmetric encryption strength respectively, are employed for RSA Key Wrapping and Diffie-Hellman Key Agreement.

7. Self Tests

The cryptographic module performs both power-up and conditional self tests to verify the integrity and correct operational functioning of the encryptor. Any failure of a self test will cause the module to transition to an error state and block all traffic on the data ports. Table 16 summarizes the module's self tests.

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. No CSPs, plaintext data, or other information, that if misused could lead to a compromise, is passed to the status output interface.

Table 16 Self Tests

Self Test	Description
Mandatory Tests	**Performed at power-up and on demand**
Known Answer Tests	Each cryptographic algorithm, employed by the encryptor, is tested using a "Known Answer Test" to verify the operation of the function. The following cryptographic algorithms are tested: AES (encrypt / decrypt), Triple-DES (encrypt / decrypt), SHA-1, SHA-256, SHA-512, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512, RSA (Sign and Verify) and ANSI X9.31 RNG.
Firmware Integrity Test	An Error Detection Code (20-byte SHA-1 hash) is used to verify the integrity of all components within the cryptographic firmware when the module is powered up.
Bypass Test	The module supports alternating between Bypass and Encrypt modes (which can be seen from the management interface). The session table contains settings, configured administratively, for Bypass mode. With each change to the session table, the module generates a checksum (32 bit CRC) and stores it as a parameter to the table. On power-up, the module calculates a fresh checksum and compares it to the stored value. If the values do not match, the module determines that an error exists within the session table; the module sets an alarm and blocks all traffic on the data ports. If the values do match, the module is assured that the session table rules have not been corrupted or erroneously changed. Any user change (crypto officer) from encrypt to bypass or vice versa shall cause an audit log entry.
Critical Functions	**Performed at power-up**
Configuration Memory	An EDC is calculated on all configuration memory and compared against the expected value, which is also stored in the configuration memory, to verify the configuration memory integrity. If the integrity check fails, the module attempts to correct the EDC and reports the failure.
Real Time Clock	The real time clock is tested for a valid time and date. If this test fails, the time and date are set to 00:00 and 01-Jan-1996 respectively.
Battery	The battery voltage 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 fails, the battery low alarm condition is raised. The module continues to operate after taking whatever precautions are necessary to guarantee correct operation. Battery alarm indication is available to all user roles via the alarm

Self Test	Description
	mechanism. This condition requires a return to factory remedy as the battery is not a user serviceable item.
General Purpose Memory	A destructive test verifies that the general purpose memory (RAM) is operating properly. The module confirms that 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 a Tamper Condition.
Conditional Tests	**Performed, as needed, during operation**
Bypass Test	The module supports alternating between Bypass and Encrypt modes. The session table contains settings, configured administratively, for Bypass mode. With each change to the session table, the module generates a checksum (32 bit CRC) and stores it as a parameter to the table. On change, the module calculates a fresh checksum and compares it to the stored value. If the values do not match, the module determines that an error exists within the session table; the module sets an alarm and blocks all traffic on the data ports. If the values do match, the module is assured that the session table rules have not been corrupted or erroneously changed.
Pair-wise Consistency	Public and private keys are used for the calculation and verification of digital signatures and for key transport. These keys are tested for consistency, based to their purpose, at the time they are generated. Encryption keys are tested by an encrypt/decrypt pair-wise consistency test; signature keys are tested by a sign/verify pair-wise consistency test.
Firmware Load	The module verifies the authenticity of any firmware load that is applied to the encryptor in the field. Only firmware loads with a valid and verified RSA signature are accepted.
Continuous RNG	The Continuous RNG test is a “stuck at” test that checks the RNG output data for failure to a constant value. Both RNGs (approved and non-approved) are subject to this test.

Crypto Officers can run the power-up self-test on demand by issuing a module reboot command. This may be accomplished via CypherManager, the Local Console, or by cycling the power to the module. Use of the Local Console or power cycling the module requires a direct connection or physical access to the module respectively. Rebooting or power cycling the module causes the keys securing the configured connections to be re-established following the restoration of communications.

8. Crypto-Officer and User Guidance

This section provides information for Crypto Officers to install, configure and operate the CN1000 Fibre Channel Encryptor in FIPS mode.

As outlined in this Security Policy, Crypto Officers (more specifically, Administrators and Supervisors) are the only administrators/operators that can make configuration changes or modify the system settings. The Crypto Officer is responsible for the physical security inspection. The only "Users" of the module are the far end encryptors which cannot modify settings. This guidance, therefore, is focused on the CO.

The CN1000 Fibre Channel Encryptor is designed to operate in either a FIPS approved mode or a non-FIPS approved mode. The operator can query the FIPS status (operating mode) of a module, and authorized operators may change the FIPS mode of operation. The FIPS status can be queried from the Local Console via the CLI or remotely via CypherManager.

To ensure that no CSPs are accessible from a previous operating mode an Erase Module and Reboot is automatically performed upon mode change.

Note: The non-FIPS mode of operation is provided for interoperability with legacy systems. The module must be configured to operate in a specific mode.

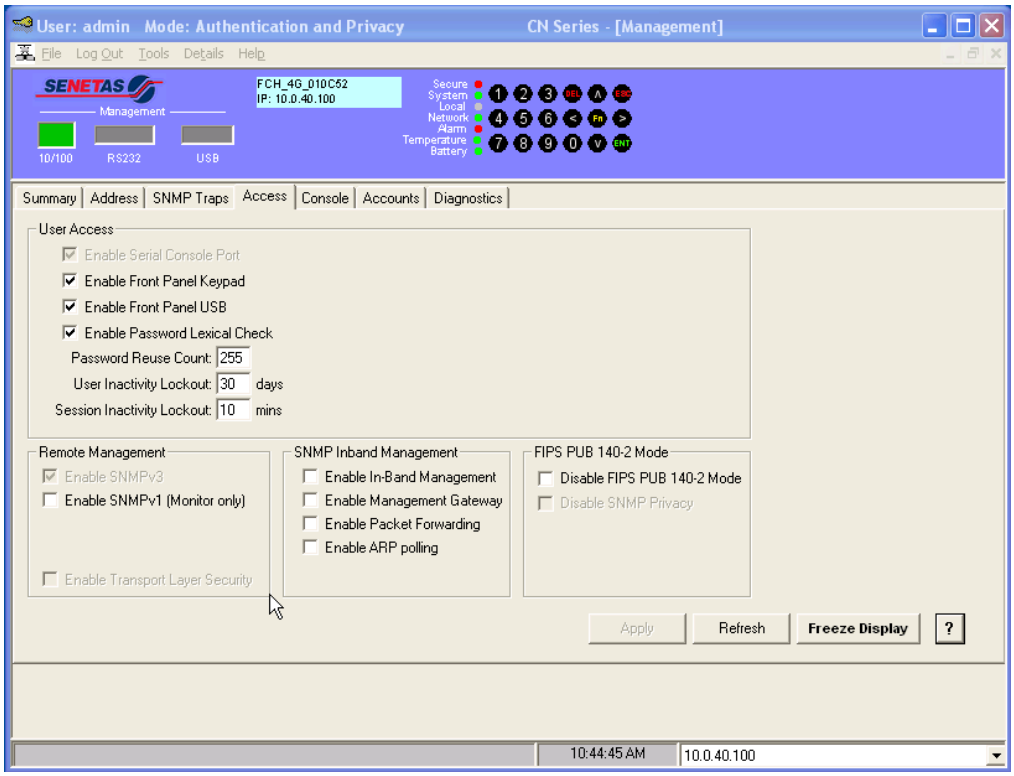
The console command is:

```
>> fips <ENTER>
```

```
CN1000 Encryptor> fips

FIPS mode enabled
```

The CypherManager screen for reporting the FIPS status is found on the User Management screen, in the Access tab.



Note: Read all of the instructions in this section before installing, configuring, and operating the CN1000 Fibre Channel Encryptor.

8.1 Delivery

When the CN1000 Fibre Channel Encryptor is delivered, the CO can verify that the model and serial numbers on the outside of the packaging, the model and serial numbers attached to the encryptor itself, and the numbers listed on the order acknowledgement, all match. The CO can also verify that the encryptor has not been modified by examining the tamper evident seal on the outside of the unit. If the seal is broken, then the integrity of the encryptor cannot be assured and Senetas should be informed immediately.

Upon receipt of the CN1000 Fibre Channel Encryptor, the following steps should be undertaken:

1. Inspect the shipping label as well as the label on the bottom of the system to ensure it is the correct FIPS approved version of the hardware.
2. Inspect the encryptor for signs of tampering. Check that the tamper evident tape and the covers of the device do not show any signs of tampering. If tampering is detected, return the device to the manufacturer.

Do not install the encryptor if it shows signs of tampering or has an incorrect label. Contact your organization's Security Officer for instructions on how to proceed.

If the device has the correct label and shows no signs of tampering, proceed to the next section.

8.2 Location

The encryptor must be installed in a secure location to ensure that it cannot be physically bypassed or tampered with. Ultimately the security of the network is only as good as the physical security around the encryptor.

Always maintain and operate CN1000 Fibre Channel Encryptor in a protected/secure environment. If it is configured in a staging area, and then relocated to its operational location, never leave the unit unsecured and unattended.

Ideally the encryptor will be installed in a climate-controlled environment with other sensitive electronic equipment (e.g. a telecommunications room, computer room or wiring closet). The encryptor can be installed in a standard 19-inch rack or alternatively mounted on any flat surface. Choose a location that is as dry and clean as possible. Ensure that the sides of the encryptor are unobstructed to allow a good flow of air through the fan vents.

The encryptor is intended to be located between a trusted and an untrusted network. The Local Interface of the encryptor is connected to appropriate equipment on the trusted network and the Network Interface of the encryptor is connected to the untrusted (often public) network.

Depending on the topology of your network, the Local Interface will often connect directly to a router, switch, or Add/Drop Multiplexer, while the Network Interface will connect to the NTU provided by the network carrier.

8.3 Configuration

Full configuration instructions are provided in the **User Manual**. Use the guidance here to constrain the configuration so that the device is not compromised during the configuration phase. This will ensure the device boots properly and enters FIPS 140-2 approved mode.

When powering up the module for the first time, use the front panel to configure the system for network connectivity. Then use CypherManager to initialize the module and perform the configuration operations.

1. Power on the unit.

   The system bootup sequence is entered each time the module is powered on and after a firmware restart. CN1000 automatically completes its self tests and verifies the authenticity of its firmware as part of the initialization process. The results of these tests are reported on the front panel LCD and are also logged in the system audit log.

   If errors are detected during the diagnostic phase, the firmware will not complete the power up sequence but will instead enter a fatal shutdown state indicating it has been tampered. If

this is the case the first time the system is powered on, the system must be returned for inspection and repair.

2. Follow the User Manual's **Installation** section to set the system's IP Address, Date and Time.
3. If CypherManager is being run for the first time, it will ask if the installation will act as the Certification Authority (CA) for the secure network. If the user selects yes a private and public RSA key pair that will be used to sign X.509 certificates is generated..

4. Install the X.509 certificate into the cryptographic module.

   The process to install a certificate is as follows:

   1. The administrator clicks the **Get Certificate** button in the CypherManager **Install New Certificate** screen. The CN1000 Fibre Channel Encryptor returns a certificate containing its public key and name. The information returned is hashed and the hash value is displayed as the validation code.
      Note: For the initial certification CN1000 must be placed in **Certificate Mode** via the front panel. Subsequent recertification does not require CypherNET to be placed in Certification Mode.
   2. After verification of the validation code the administrator must enter the private key password (used to secure the local CypherManager database) and the new administrator account details for CN1000.
   3. After the administrator clicks the **OK** button CypherManager signs the X.509 certificate and sends it back to the CN1000. The contents of the certificate are hashed and the hash value is displayed as the validation code.
      Note: On initial certification the certificate must be accepted on CN1000 to complete installation.
   4. The administrator must then log out of the CN1000 being managed and log back in using the new administrator account details.

   After an X.509 certificate has been installed into CN1000 the administrator can create supervisor and operator accounts.

   At this point the CN1000 is able to encrypt in accordance with the configured security policy; the ENT key on the front panel is disabled; and the default factory account has been removed.
5. Ensure the encryptor is in FIPS 140-2 mode (default setting) via the CypherManager **User Management Access** tab;
6. Configure the security policy to enable encrypted tunnels with other CN1000 units.

   Configuration of the security policy is network specific; refer to the User Manual for specific details.

9. Mitigation of Other Attacks

The module does not mitigate specific attacks.

End