Senetas Corporation Ltd, distributed by Gemalto NV (SafeNet)

Module Name(s):	**CN9000 Series Encryptors**
Model Names:	**CN9100 100G Ethernet Encryptor**
	CN9120 100G Ethernet Encryptor
Module Version:	**CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC), A9122B (AC/DC)**

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

June 2019

CN9100 Encryptor
Senetas Corp. Ltd & SafeNet Co-branded

CN9100 Encryptor
Senetas Corp. Ltd Sole branded

CN9120 Encryptor
Senetas Corp. Ltd & SafeNet Co-branded

CN9120 Encryptor
Senetas Corp. Ltd Sole branded

Table of Contents

1. Introduction 3
   1.1 References 3
   1.2 Document History 4
   1.3 Acronyms and Abbreviations 4
2. Product Description 6
   2.1 Module Identification 7
   2.2 Operational Overview 8
      2.2.1 General 8
      2.2.2 Encryptor deployment 9
      2.2.3 Encryptor management 10
      2.2.4 Ethernet implementation 11
3. Module Ports and Interfaces 13
   3.1 CN9000 Series Ports 13
   3.2 CN9000 Series Interfaces 17
4. Administrative Roles, Services and Authentication 20
   4.1 Identification and Authentication 21
   4.2 Roles and Services 22
5. Physical Security 25
6. Cryptographic Key Management 27
   6.1 Cryptographic Keys and CSPs 27
   6.2 Key and CSP zeroization 36
      6.2.1 Zeroization sequence 36
      6.2.2 Erase command and key press sequence 36
      6.2.3 Approved mode of operation 36
      6.2.4 Tamper initiated zeroization 37
      6.2.5 Emergency Erase 37
   6.3 Data privacy 37
   6.4 Cryptographic Algorithms 38
   6.5 Key Derivation Functions 41
   6.6 Non Approved and Allowed Security Functions 41
7. Self Tests 44
8. Crypto-Officer and User Guidance 47
   8.1 Delivery 48
   8.2 Location 48
   8.3 Configuration – FIPS140-Approved mode 48
   8.4 Configuration - Non-Approved Mode 50
9. Mitigation of Other Attacks 50

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the Senetas Corporation Ltd. CN9000 Series Encryption devices currently comprising of two models the CN9100 and the CN9120 (version 3.0.3). This Security Policy specifies the security rules under which the module operates to meet the FIPS 140-2 Level 3 requirements.

The CN9000 Series of Ethernet Encryption devices are distributed worldwide under different brands as depicted in this Security Policy. The vendor distributes under their Senetas brand and Gemalto NV, the master worldwide distributor, distributes under the joint SafeNet/Senetas brand.

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/CSE 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 CN9000 Series comply with the eleven sections of the standard. In this document, CN9100 and CN9120 Encryptors are collectively referred to as the “CN9000 Series” and individually as “the module” or “the encryptor”.

This Security Policy and the associated CMVP certificate are for firmware version 3.0.3 only – the loading of any other firmware version on the specified CN9000 Series Ethernet Encryption devices is out of scope of this FIPS 140-2 validation.

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 CN9000 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 .

[1] *FIPS PUB 140-2: Security Requirements for Cryptographic Modules.*

[2] *FIPS 140-2 Annex A: Approved Security Functions.*

[3] *FIPS 140-2 Annex B: Approved Protection Profiles.*

[4] *FIPS 140-2 Annex C: Approved Random Number Generators.*

[5] *FIPS 140-2 Annex D: Approved Key Establishment.*

[6] *NIST Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*

[7] *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.*

[8] *Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197.*

[9] *Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2.*

[10] *Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4.*

[11] *NIST Special Publication (SP) 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*

[12] *NIST Special Publication (SP) 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit GeneratorsNIST.*

[13] *NIST Special Publication (SP) 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.*

[14] *Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4.*

[15] *NIST Special Publication (SP) 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography.*

1.2 Document History

Authors	Date	Version	Comment
Senetas Corporation Ltd.	05-May-2017	1.00	Senetas CN9000 Release v3.0.1
Senetas Corporation Ltd.	01-Aug-2017	1.01	Updates to address CSC comments
Senetas Corporation Ltd.	12-Oct-2017	1.02	Updates to address CMVP comments
Senetas Corporation Ltd.	28-Nov-2017	1.03	CMVP final v3.0.1/3.0.2 Security Policy
Senetas Corporation Ltd.	22-Jan-2018	1.04	Changes to address non-compliant AES key wrapping
Senetas Corporation Ltd.	31-Jan-2018	1.05	Updates to address CMVP comments
Senetas Corporation Ltd.	19-Oct-2018	1.10	Senetas v3.0.3 firmware release
Senetas Corporation Ltd.	24-Jun-2019	1.11	Updates to address CMVP comments

1.3 Acronyms and Abbreviations

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CFP4	C Form-factor Pluggable (transceiver)
CM7	Senetas Encryptor Remote Management Application Software
CI	Connection Identifier (used interchangeably with Tunnel)
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter Mode
CRNGT	Continuous Random Number Generator Test
DEK	Data Encrypting Key(s)
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FTPS	FTP Secure (FTP Over TLS)
Gbps	Gigabits per second
GEK	Group Establishment Key

HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
KEK	Key Encrypting Key(s)
LED	Light Emitting Diode
MAC	Media Access Control (Ethernet source/destination address)
Mbps	Megabits per second
NIST	National Institute of Standards and Technology
NTU	Network Termination Unit
NVLAP	National Voluntary Laboratory Accreditation Program
OAEP	Optimal Asymmetric Encryption Padding
PKCS	Public Key Cryptography Standards
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
RTC	Real Time Clock
SAN	Storage Area Network
SDRAM	Synchronous Dynamic Random Access Memory
SFTP	Secure FTP over SSH
SID	Sender ID
SMC	Gemalto’s Network Security Management Center
SME	Secure Message Exchange
SMK	System Master Key
SP	Special Publication
SHA	Secure Hash Algorithm
SSH	Secure Shell
TACACS+	Terminal Access Control Access Control Server
TRANSEC	TRANsmission SECurity (also known as Traffic Flow Security or TFS)
TLS	Transport Layer Security
X.509	Digital Certificate Standard RFC 2459

2. Product Description

CN9000 Series Encryptors are multiple-chip standalone cryptographic modules consisting of production-grade components contained, in accordance with FIPS 140-2 Level 3, in a physically protected enclosure. The module's outer casing defines the cryptographic boundary aside from the pluggable transceivers (CFP4 on the CN9100 and QSFP28 on the CN9120), dual redundant power supplies and replaceable fan tray module that lie outside the crypto boundary. All ventilation holes are protected by steel anti-probing barriers. The encryptor is enclosed in a steel and aluminium case which is protected from tampering by internal tamper protection circuitry and external tamper evident 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

2.1 Module Identification

CN9000 Series Encryptors, with firmware version 3.0.3, provide data privacy and access control services for Ethernet 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 CN9000 Models: Hardware/Firmware Versions

Hardware Versions	Power	Interface / Protocol (Cryptographic Module)	Firmware Version
A9100B [O][1,2] A9100B [Y][1,2]	AC	100G Ethernet	3.0.3
A9101B [O][1,2] A9101B [Y][1,2]	DC		
A9102B [O][1,2] A9102B [Y][1,2]	AC/DC		
A9120B [O][1,3] A9120B [Y][1,3]	AC	100G Ethernet	3.0.3
A9121B [O][1,3] A9121B [Y][1,3]	DC		
A9122B [O][1,3] A9122B [Y][1,3]	AC/DC		

Table Notes:

Note 1: Model variants distinguished by [O] and [Y] are identical except for logos on the front fascia:

[O] Denotes Senetas Corp. Ltd. sole branded version

[Y] Denotes Senetas Corp. Ltd. & SafeNet co-branded version

Note 2: This model supports pluggable CFP4 transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Note 3: This model supports pluggable QSFP28 transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Safenet/Senetas Co-branding **Senetas Sole Branding**

Figure 1 – Senetas/SafeNet co-branding

2.2 Operational Overview

2.2.1 General

CN9000 Series Encryptors operate in point-to-point and point-to-multipoint network topologies and at a data rate of 100Gb/s.

Encryptors are typically installed between an operator's private network equipment and public network connection and are used to secure data travelling over either fibre optic cables.

Securing a data link that connects two remote office sites is a common installation application.
Figure 2 provides an operational overview of two CN9000 Series encryptors positioned in the network.

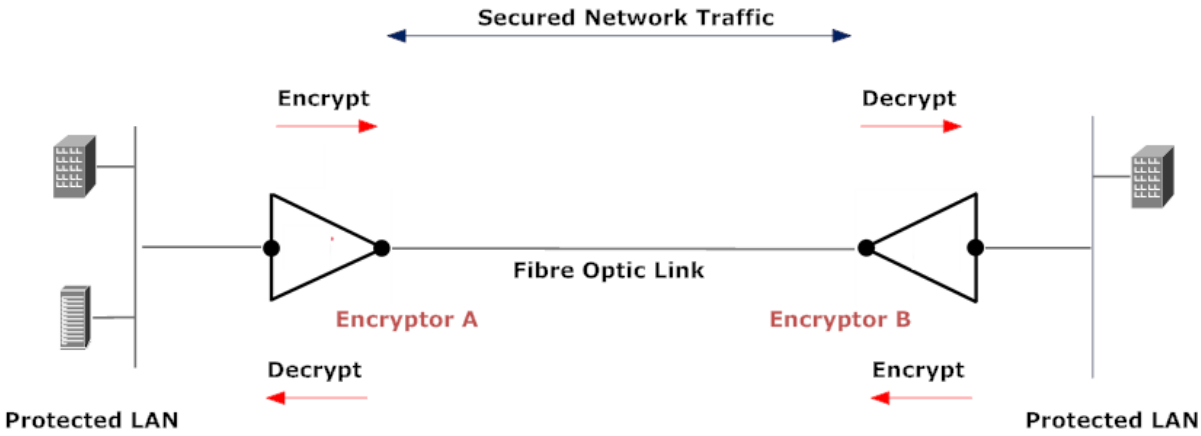

Figure 2 – CN9000 Series Operational Overview

Devices establish one or more encrypted data paths referred to as `connections`. The term refers to a connection that has been securely established and is processing data according to a defined encryption policy. Each `connection` has a `connection identifier` (CI) and associated CI mode that defines how data is processed for each policy. Connections are interchangeably referred to as 'tunnels'.

CN9000 Series Encryptors support CI Modes of 'Secure', 'Discard' and 'Bypass'. These CI Modes can be applied to all data carried on a connection or to a selected subset or grouping which can be user configured in accordance the specific protocol being carried on the network connection. A typical example in the case of an Ethernet network would be to make policy decisions based upon an Ethernet packet's VLAN ID.

The default CI Mode negotiated between 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 the key encrypting key (KEK) and initial data encryption key (DEK), using the RSA-OAEP-256 key transport process in accordance with NIST SP800-56B. Alternatively, ECDSA/ECDH utilises ephemeral key agreement for the purpose of establishing DEKs in accordance with NIST SP800-56A. If the session key exchange is successful this results in a separate secure session per connection, without the need for secret session keys (DEKs) to be displayed or manually transported and installed.

Figure 3. illustrates the conceptual data flow through a CN9000 Series Encryptor.

1. A data packet arrives at the encryptor's interface ports. When operating in Line mode data packets are processed according to a single CI policy, otherwise,
2. The encryptor looks up the appropriate packet header field, e.g. VLAN ID and determines whether the field has been associated with an existing CI,
3. If a match is found, the encryptor will process the data packet according to the policy setting for that CI and send the data out the opposite port. If a match cannot be found, the data packet is processed according to the default policy setting.

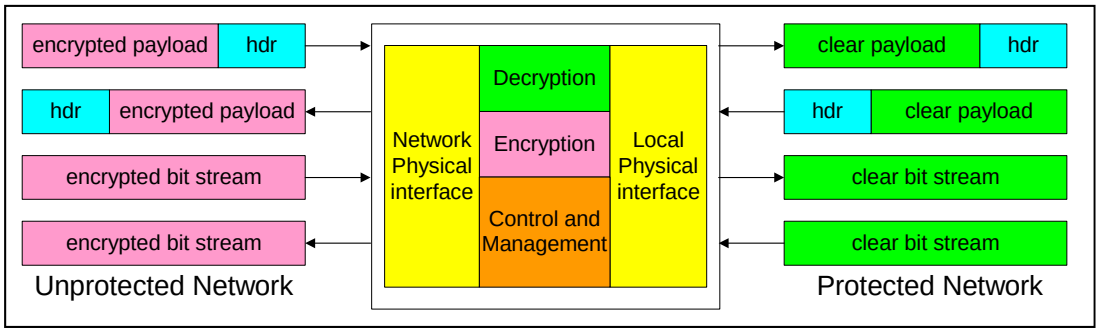

Figure 3 - Data Flow through the Encryptor

2.2.2 Encryptor deployment

Figure 4 illustrates a point-to-point (or link) configuration in which each module connects with a single far end module and encrypts the entire bit stream. If a location maintains secure connections with multiple remote facilities, it will need a separate pair of encryptor's for each physical connection (link).

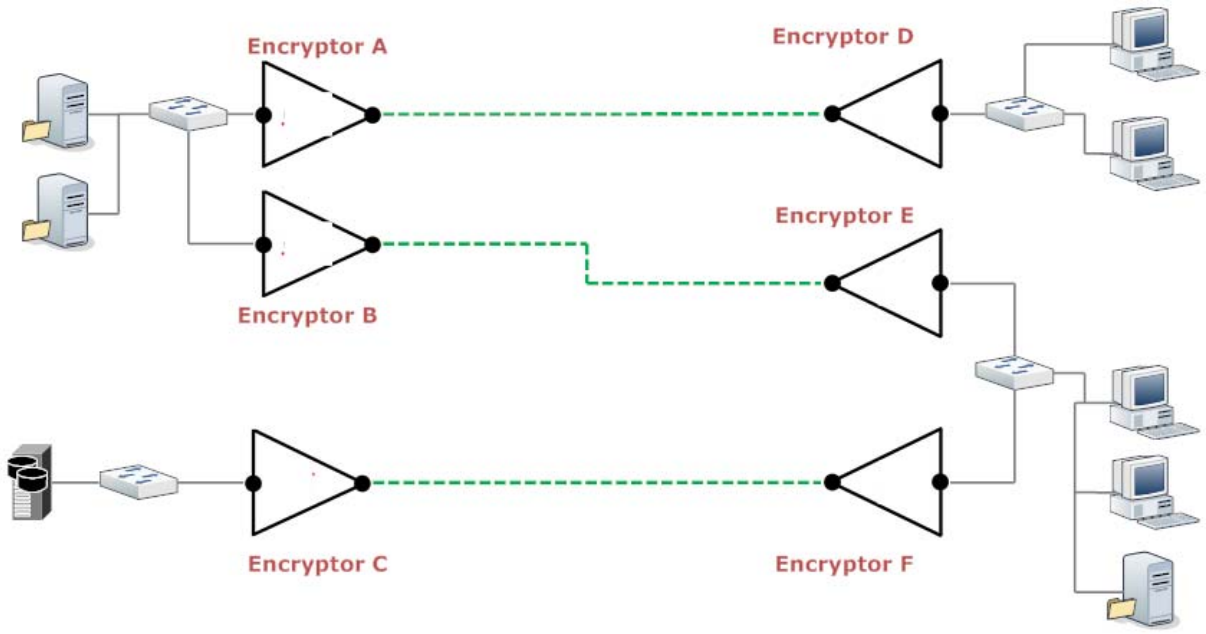

Figure 4 - Link Configuration

Figure 5 illustrates a meshed network configuration. Each CN9000 Series Encryptor is able to maintain simultaneous secured connections with many far end encryptors.

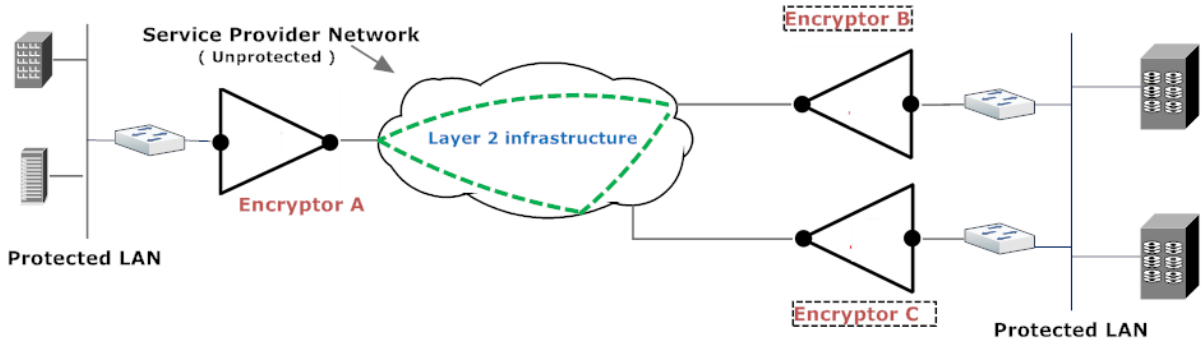

Figure 5 - Meshed Configuration

2.2.3 Encryptor management

Encryptors can be centrally controlled or managed across local and remote stations using the CM7 or SMC remote management application. The remote management applications reside outside the cryptographic boundary and are not in the scope of the FIPS validation. 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. Alternatively the CLI can be accessed remotely via SSH (when configured). The authentication algorithm for remote cli access is restricted to RSA and ECDSA. RSA Keys must be a minimum of 2048 bits and ECDSA keys are restricted to NIST P-256, P-384 and P-521 curves. Remote cli access is disabled by default.

FIPS-Approved mode of operation enforces the use of SNMPv3 privacy and authentication. Management messages are encrypted using AES-128. Non-Approved mode allows message privacy to be disabled in order to interwork with 3rd party legacy management applications.

2.2.4 Ethernet implementation

Basic operation

The Ethernet encryptor provides layer 2 security services by encrypting the contents of data frames across Ethernet networks. The encryptor connects between a local (protected) network and a remote (protected) network across the public (unprotected) network. An encryptor is paired with one or more remote Ethernet encryptors to provide secure data transfer over encrypted connections as shown in Figure 6 below.

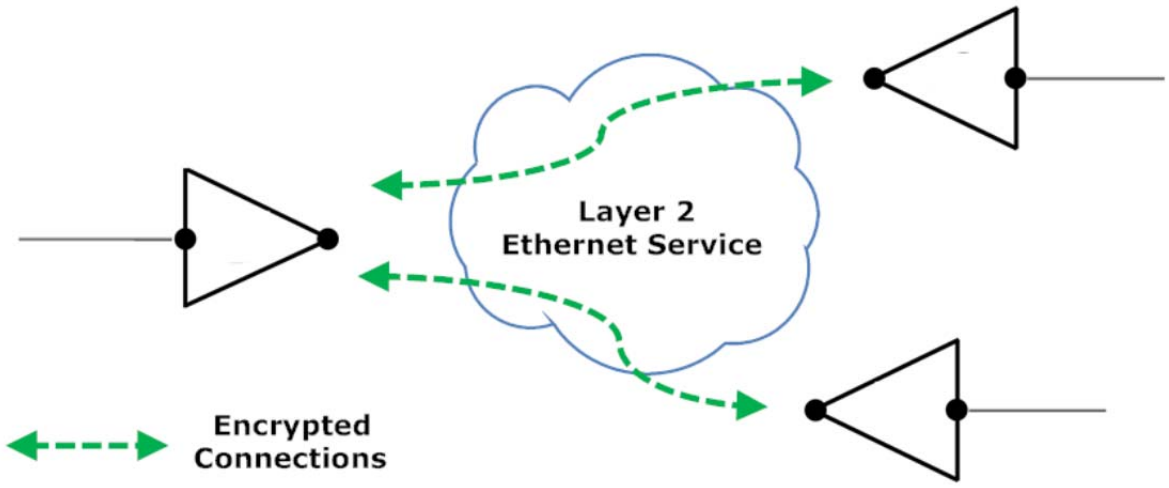

Figure 6 – Layer 2 Ethernet connections

The encryptor's Ethernet receiver receives frames on its ingress port; valid frames are classified according to the Ethernet header then processed according to the configured policy.

Allowable policy actions are:

- Encrypt – payload of frame is encrypted according to the defined policy
- Discard – drop the frame, no portion is transmitted
- Bypass – transmit the frame without alteration

CN9000 Series tunnels are encrypted using CAVP validated AES algorithms. The CN9000 Series 100G Ethernet encryptors support AES encryption with a key size of 128 or 256 bits in counter (CTR) mode.

Connections between encryptors use a unique key pair with a separate key for each direction.

The Ethernet transmitter module calculates and inserts the Frame Check Sequence (FCS) at the end of the frame. The frame is then encoded and transmitted. For details about Unicast and Multicast network topologies supported by the modules see next section.

Unicast operation

Unicast traffic is encrypted using a key pair for each of the established connections.

When operating in line mode there is just one entry in the connection table. When operating in multipoint mode, connection table entries are managed by VLAN ID and can be added manually, or if 'Auto discovery' is enabled, they will be automatically added based on the observed traffic. Entries do not age and will remain in the table.

Multipoint VLAN operation

Multicast traffic between encryptors connected in line mode shares the same single key pair that is used by unicast traffic.

VLAN encryption mode is used to encrypt traffic sent to all encryptors on a VLAN. Unlike unicast encryption (which encrypts traffic from a single sender to a single receiver and uses a unique pair of keys per encrypted connection), VLAN encryption within a multipoint network requires a group key management infrastructure to ensure that each encryptor can share a set of encryption keys per VLAN ID. The group key management scheme which is used for VLAN mode is responsible for ensuring group keys are maintained across the visible network.

The group key management scheme is designed to be secure, dynamic and robust; with an ability to survive network outages and topology changes automatically. It does not rely on an external key server to distribute group keys as this introduces both a single point of failure and a single point of compromise.

For robustness and security a group key master is automatically elected amongst the visible encryptors within a mesh based on the actual traffic.

If communications problems segment the network, the group key management scheme will automatically maintain/establish new group key managers within each segment.

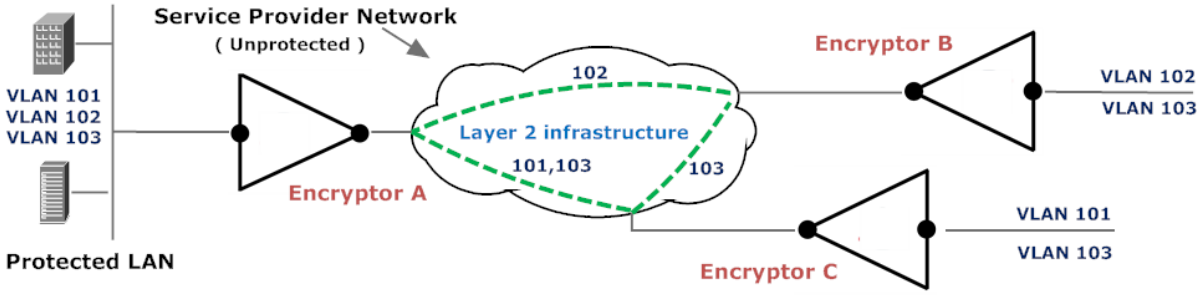

Figure 7 – Multipoint VLAN connections

3. Module Ports and Interfaces

3.1 CN9000 Series Ports

The CN9000 Series data and management ports are located on the encryptor's front panel.

The encryptor's data ports include a Local Port which connects to the physically secure private network and the Network Port which connects to an unsecured public network.

The encryptor's user access management ports, LCD display and Keypad are located on the front of the module as presented in Figure 8 and Figure 9 below.

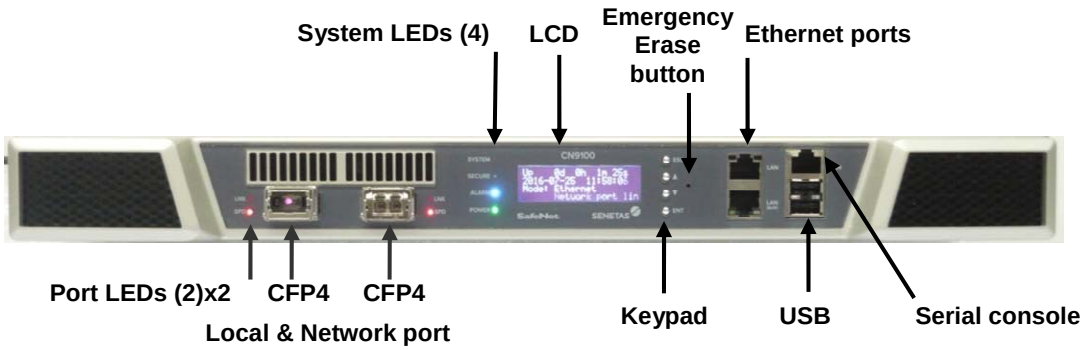

Figure 8 - Front View of the CN9100 [Y] Encryptor

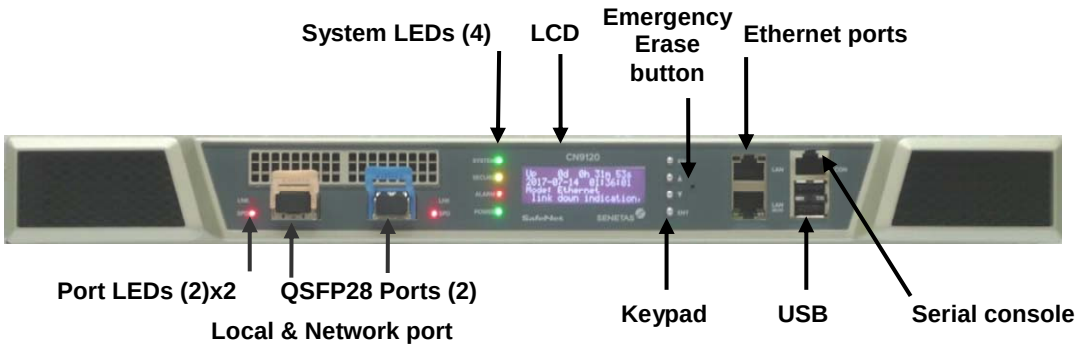

Figure 9 - Front View of the CN9120 [Y] Encryptor

CN9000 Series Encryptors support dual redundant power supplies which are available in two variants, an AC version for typical installs and a DC version for telecoms applications. Any power supply combination i.e. AC/AC, AC/DC or DC/DC is supported. Details of each can be seen in Figure 10.

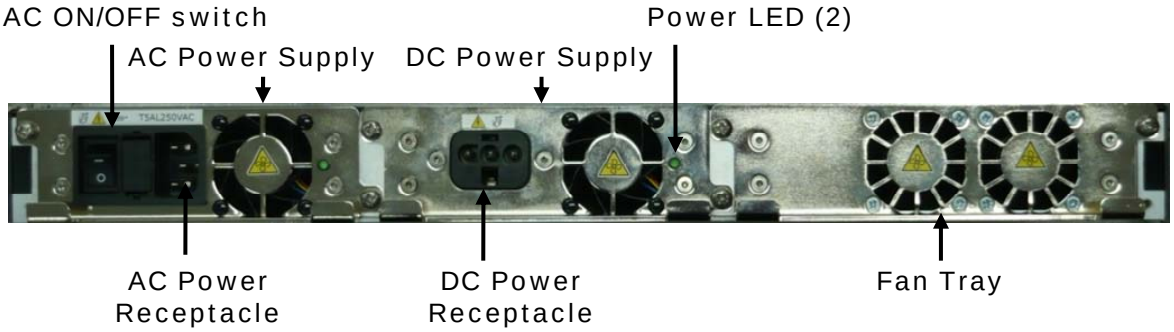

Figure 10 - Rear View: CN9000 Series Encryptor

Figure 11 – A9100B 100G Ethernet ports close-up - CFP4s not installed

Figure 12 – A9100B 100G Ethernet ports close-up - CFP4s installed

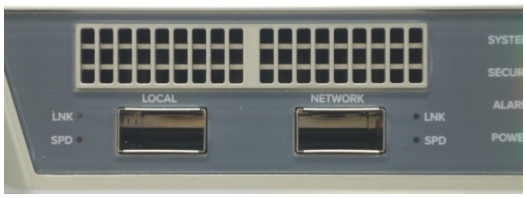

Figure 13 – A9120B 100G Ethernet ports close-up – QSFP28s not installed

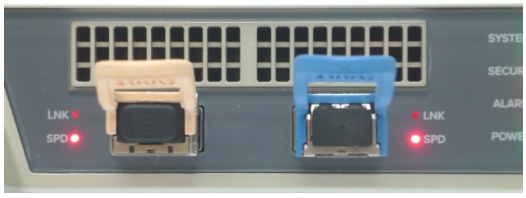

Figure 14 – A9120B 100G Ethernet ports close-up - QSFP28s installed

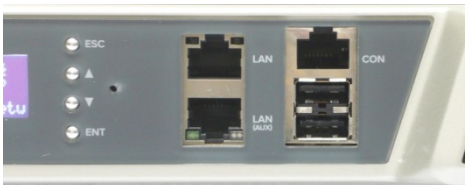

Figure 15 – CN9000 Series RJ45 Ethernet, Console and USB close-up

Table 3 defines the Physical Ports.

Table 3 CN9000 Series Physical Ports

Port	Location	Purpose
RJ-45 Ethernet	Front Panel (LAN)	Allows secure and authenticated remote management by the selected remote management application.
RJ-45 Ethernet	Front Panel (AUX)	Not enabled and physically blocked - port reserved for future use.
RJ-45 RS-232 Console	Front Panel	The Serial Console port connects to a local terminal and provides a simple command line interface (CLI) 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 a mechanism for applying approved and properly signed firmware upgrades 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 any operational alarm states.
System LEDs	Front Panel	Indicate the system state, including secure status, alarms and power.
Port LEDs	Front Panel	Indicate local and network port status and activity.
Network Port	Front Panel	The Network Port connects to the public network; access is protected by X.509v3 certificates. The Network Port is of the same interface type as the Local Port.
CN9100		CFP4 socket[1]
CN9120		QSFP28 socket[2]
Local Port	Front Panel	The Local Port connects to the private network; access is protected by X.509v3 certificates. The Local Port is of the same interface type as the Network Port.
CN9100		CFP4 socket[1]
CN9120		QSFP28 socket[2]
Emergency Erase button	Front Panel	The concealed front panel Emergency Erase button can be activated using a paperclip or similar tool and will immediately delete the System Master Key. The Emergency Erase button functions irrespective of the powered state of the module.

Port	Location	Purpose
Power Connectors	Rear Panel	Provide AC power to the module depending upon which power modules have been installed
Power LEDs	Rear Panel	Indicates whether power module is ON or OFF.

Note 1: The CFP4 sockets are the receptacles for the pluggable CFP4 optical transceivers.

Note 2: The QSFP28 sockets are the receptacles for the pluggable QSFP28 optical transceivers.

3.2 CN9000 Series 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	CN9000 Series 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	RJ-45 RS-232 Serial Console
	Keypad & Display	Keypad / LCD
	Remote Management Interface	Management RJ-45 Ethernet Port (LAN)
	Private Network Interface	Local Port
	Public Network Interface	Network Port
	Emergency Erase button	Emergency Erase button
	USB Firmware Upgrade	USB Port
Status Output	Local Console	RJ-45 RS-232 Serial Console
	Keypad & Display	Keypad / LCD
	Remote Management Interface	Management RJ-45 Ethernet Port (LAN)
	Private Network Interface	Local Port
	Public Network Interface	Network Port
	LEDs	Front & Rear LEDs
Power	Power Switch	Power Connector

CN9000 Series Encryptors support 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 or ECDSA/ECDH 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 the Remote Management Interface as follows: • The Keypad supports module initialization prior to authentication and operation in the approved mode. A Crypto Officer sets the IP address for administration by the remote management application; sets the system clock; and loads, in conjunction with the remote management application, 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 remote management 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 remote management 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 the 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 X.509v3 certificates. • The System LEDs indicate the system and tunnel state as well a combined alarm status covering network and local ports. • The Port LEDs indicate the state of the local and network interfaces and the presence of 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 remote management 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 remote management application by way of the Local or Network Port rather than the RJ-45 Ethernet

Logical Interface	Support
	Port.

The encryptor does permit logically distinct categories of information to share the Local and Network Ports. For example, when the module is configured to allow in-band management traffic, the control/status information (key exchange or management commands) and user data enter and exit the module via the Network Interface. The module separates these two logically distinct categories of information by applying a unique vendor specific Ethertype and separate subtypes to management packets and key exchange messages.

4. Administrative Roles, Services and Authentication

The cryptographic module supports four administrative privilege levels: Administrator, Supervisor, Operator and Upgrader. The Administrator role is highest (most unrestricted) privilege level and is authorized to access all module services. FIPS140-2 defines two operator classes, the Crypto Officer, who is granted access to management functions and the User who obtains cryptographic services of the module. Crypto Officers would assume the role of either an Administrator or Supervisor whilst Users can assume the role of an Operator or Upgrader.

The supported roles are summarized in Table 7.

Table 7 Roles

Operator Class	Role
Crypto Officer	**Administrator:** Provides cryptographic initialization and management functions. Crypto Officer functions are available via the CM7 or SMC remote management application. Limited functions are also available via the Console interface. **Supervisor:** Provides limited operational management functions. Functions are available via the remote management application. 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 Remote Management Interface and the remote management application.
User	Restricted to read-only access to module configuration data. **Operator:** The Operator role is intended to provide sufficient restricted module access for an IT professional to monitor and ensure the network infrastructure to which the encryptor is connected is intact and operational. Services for the Operator are accessible directly via the Local Console CLI or remotely via the Remote Management Interface and the remote management 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 remote management application.

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. Remote 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 operators.

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 using several methods. When the module is powered on, the module can be zeroized by executing the Erase command or by performing the front panel Erase key press sequence defined in the user manual. An immediate erase can be achieved, powered or un-powered, by depressing the concealed front panel Emergency Erase button, accessed using a "paperclip" or other suitable tool. Refer to Figure 8 for location.

4.1 Identification and Authentication

The module employs Identity-Based Authentication. The module also supports TACACS+ for authentication in FIPS non-Approved mode only. Four operator privilege levels have been defined for use, Administrator, Supervisor, Operator and Upgrader with access rights as indicated in Table 8. Restricted Administrator privileges are available until the module is “Activated”. Activation ensures that the default Administrator password is changed and allows additional user accounts to be created. A user with Administrator privilege can further restrict the available privilege levels to Administrator and Operator by selecting “Simplified” user model from the CLI.

Users with administrator privilege level can set a password change lockout period of between 0 (disabled) and 240 hours in which user’s passwords cannot be changed. This feature is intended to prevent a user from exhausting the password history and recycling a previously used password. The feature is disabled by default.

Up to 30 user accounts with unique names and passwords may be defined for authorised operators (Administrators, Supervisors Operators and Upgraders) of the module. Operators using the Local Console enter their name and password to authenticate directly with the module. Operators using the remote management application issue commands to the encryptor. Password based authentication is used between the management station and the module to authenticate each user. If the user is authenticated then Diffie-Hellman Key Agreement is employed to establish secure AES SNMPv3 privacy keys allowing the transport of secure messages to and from the module. Commands from the remote management application 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 Certificate Authority (CA). The modules exchange Key Encryption Keys and Data Encryption keys using RSA-OAEP-256 public key transport in accordance with NIST SP800-56B (subsequent DEKs are transferred using AES key wrapping authenticated with HMAC-SHA256 in accordance with the IG D.9). Alternatively, ECDH ephemeral key agreement is used for the purpose of establishing DEKs in accordance with NIST SP800-56A.

Table 8 Authentication Type

Role	Type of Authentication	Authentication Data
Administrator **Supervisor** **(Crypto Officers)**	Identity-based	Crypto Officers using the Local Console present unique user names and passwords to log in to the CLI. Crypto Officers using the remote management application have unique identities embedded in the command protocol. Each issued command is individually authenticated.
Operator **Upgrader** **(Users)**	Identity-based	Users follow the same authentication rules as Crypto Officers.

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

Table 9 Strength of Authentication

Authentication Mechanism	Strength
Password	Crypto Officers, 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 (218,340,105,584,896) possible combinations making the possibility of correctly guessing a password $1/62^8$ which is far 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.
Network User Certificates	Far end modules (Users) authenticate using an RSA authentication certificate based on 2048 bit keys providing 112 bit key size equivalence. Therefore the possibility of deriving a private RSA key is $1/2^{112}$ which is far less than 1 in 1,000,000. Alternatively far end modules authenticate using an ECDSA authentication certificate using NIST P-256, P-384 or P-521 may curves which provide 128, 192 and 256 bit key size equivalence respectively. The worst case probability of deriving an ECDSA private key is $1/2^{128}$ which is far less than 1 in 1,000,000. Based on the multi-step handshaking process, requiring authentication at each stage, the secure session establishment sequence ensures the possibility of randomly guessing the authentication key in 60 seconds is less than 1 in 100,000. Upon an unsuccessful authentication attempt the secure session establishment mechanism will go into a fault state that takes one minute to clear.

4.2 Roles and Services

CN9000 Series Encryptors support 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.

N/A - Not Applicable

The module's services are described in more detail in the CN9000 Series documentation. Note access to and behaviour of module services are identical when operating in FIPS-Approved or non-Approved modes.

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 10 Operator – Roles and Services

Crypto Officer		User		Authorized Service	Cryptographic Keys and CSPs	Access Type
Admin	Supv	Oper	Upgr			
✓	✓			Set Real Time Clock	none	N/A
✓				Load Module Certificate[7]	RSA or ECDSA Public and Private Keys[8] RSA or ECDSA Public Key Certificate	W
✓				Create User Account	Password	W
✓				Modify User Account	Password	E, W
✓				Delete User Account	Password	D
✓	✓	✓	✓	View User Account	none	N/A
✓	✓			Edit Connection Action Table (Bypass)	none	N/A
✓	✓	✓	✓	View Connection Action Table	none	N/A
✓	✓	✓	✓	Show Firmware Version	none	N/A
✓				Clear Audit Trail	Password	W
✓	✓	✓	✓	View Audit Trail	none	N/A
✓				Clear Event Log	Password	W
✓	✓	✓	✓	View Event Log	none	N/A
✓	✓	✓	✓	View FIPS Mode Status	none	N/A
✓				Change FIPS Mode Status	Password	W
✓	✓			Run Self Test (Reboot Command)	Password	E
✓			✓	Install Firmware Upgrade	Password Firmware Upgrade RSA Public Key	E
✓			✓	Establish FTPS (TLS) Session	FTPS (TLS) Privacy Keys[3], FTPS (TLS) Private Key, FTPS (TLS) Public Key, FTPS (TLS) HMAC keys, FTPS (TLS) Master Secret[8]	R, W, E

Crypto Officer		User		Authorized Service	Cryptographic Keys and CSPs	Access Type
Admin	Supv	Oper	Upgr			
✓			✓	Establish SFTP (SSH) Session	SFTP (SSH) Privacy Keys[3], SFTP (SSH) Key Exchange Private Keys, SFTP (SSH) Key Exchange Public Keys, SFTP (SSH) HMAC keys, SFTP (SSH) Shared Secret[8]	R, W, E
✓	✓			Re/Start Secure connection	AES KEKs[1,5], AES DEKs[1], AES GEKs[6], (DRBG Seed, DRBG V Value, DRBG Entropy Input and Nonce), SME HMAC key, ECDHE Shared Secret[8]	W
✓				Generate X.509v3 Certificate Signing Request	RSA Private Key and RSA Public Key or ECDSA Private Key and ECDH Public Key[8]	R, E
✓				Erase Module – Zeroize (Console Command)	System Master Key and all CSP data stored in non-volatile memory	D
✓	✓	✓	✓	Establish a Remote Management Session	SNMPv3 Privacy Key[2], SNMPv3 Diffie Hellman Private Keys, SNMPv3 Diffie Hellman Public Keys[8]	R, W, E
✓	✓	✓	✓	Establish a Remote CLI Session[4]	Remote CLI (SSH) Privacy Keys, Remote CLI (SSH) Key Exchange Private Keys, Remote CLI (SSH) Key Exchange Public Keys, Remote CLI (SSH) HMAC keys	R, W, E

Note 1: Starting/Restarting a secure connection causes new KEKs, DEKs GEKs and SME HMAC keys to be generated .

Note 2: AES SNMPv3 Privacy keys are established using Diffie-Hellman when an SNMPv3 remote management session is initiated and used to encrypt and decrypt all subsequent directives. The DH modulus size is set to a minimum of Oakley group 14 (2048 bits) in SNMP.

Note 3: If the firmware upgrade image is being transferred via SFTP then AES SFTP (SSH) Privacy Keys are established using either DH or ECDH. If the firmware upgrade image is being transferred via FTPS then AES FTPS (TLS) Privacy Keys are established using ECDH.

Note 4: AES Remote CLI (SSH) Privacy Keys are established using DH or ECDH when a remote CLI session is established. The DH modulus size is set to Oakley group 14 (2048 bits) in SSH. The RSA key size is checked when a user loads a remote CLI SSH key. It is rejected if it is less than 2048 bits.

Note 5: AES KEKs are established using Approved (Vendor Affirmed) RSA-OAEP-256 key transport as per NIST SP-800-56B and described in Table 13.

Note 6: AES GEKs are established using ECDH key agreement.

Note 7: The Load Module Certificate service can access any RSA or ECDSA Public/Private keys that are associated with the certificate being loaded. The RSA key size in a certificate is checked when the certificate is loaded onto the module. If the key size is below 2048 bits the certificate will be rejected.

Note 8: All key material is sourced from the SP-800-90A DRBG and in accordance with IG Section 14.5 the entropy input string and seed are considered CSPs. Note that the implementation re/instantiates on each call to the DRBG, and the value V, constant C and reseed_counter are internal to the DRBG, and cleared on each use.

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

CN9000 Series Encryptors employ 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 front panel 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 immediately causes the module to be set into 'Discard' mode and initiates the zeroization of all Keys and CSPs. For further details refer to Section 6.2.
3. Two tamper evident seals are pre-installed (at factory). Both are placed between the top cover and underside of the main enclosure (refer to Figure 16). Attempting to remove the 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. Replacement tamper seals cannot be ordered from the supplier. A module with damaged tamper evident seals should be returned to the manufacturer by the Crypto Officer.

Figure 16 – Factory installed tamper seals

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

Table 11 outlines the recommended inspection practices and/or testing of the physical security mechanisms.

Table 11 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 and physical evidence of tampering against the tamper seals. The Crypto Officer is responsible for the physical security inspection. During normal operation, the Secure LED is illuminated **green**. When the unit is not activated and/or uncertified (i.e. it has no loaded certificate since it is either in the default factory manufactured state or a 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 the 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 re-activated and re-certified.	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 12 Cryptographic Keys and CSPs

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	**Storage**	**Sourced**	**Format**		
System Master Key[6, 7]	On initialization, the module generates a 192-bit symmetric key using the NIST SP800-90A DRBG. This key encrypts, using 3-key Triple-DES CFB8, the module's private RSA and ECDSA keys and the user passwords stored in the configuration flash memory.	Internal	Plaintext, in a tamper protected memory device	No	N/A	On tamper or Erase[3.] the System Master Key is zeroized.	No
RSA Private Key(s)	A Private 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 the remote management application. The RSA Private Key(s) are used to authenticate connections with other encryptors and to unwrap master session keys (KEKs) and session keys (DEKs) received from far-end encryptors.	Internal	3-key Triple-DES-encrypted format, non-volatile system memory.	No	N/A	On tamper or Erase[3] the Triple-DES System Master Key is zeroized, rendering the encrypted RSA Private Key undecipherable. Each event also deletes the RSA keys from non-volatile memory.	No
RSA Public Key(s)	This Public 2048 bit key is the public component of a module's RSA Key pair. They reside in the Network Certificate and are used for authenticating connections with other encryptors. The module and the remote management application CM7 will only generate certificates with RSA 2048-bit key size. It is possible to load a certificate from an external CA with RSA 4096-bit key size, although the encryptor certificate will have an RSA 2048-bit key which will be used for key wrapping the KEKs.	Internal Electronic	Stored in non-volatile system memory.	Electronic	Plaintext within X.509 certificate signed by trusted CA	On tamper or Erase[3] the Triple-DES System Master Key is zeroized, rendering the encrypted RSA Public Key undecipherable. Each event also deletes the RSA keys from non-volatile memory.	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	**Storage**	**Sourced**	**Format**		
ECDSA Private Key(s)	A Private ECDSA key using NIST P-256, P-384 or P-521 curves is the secret component of the module's ECDSA Key pair. It is generated when the module receives a Load Certificate command from the remote management application. The ECDSA Private Key(s) are used to authenticate connections with other encryptors.	Internal	3-key Triple-DES-encrypted format, non-volatile system memory.	No	N/A	On tamper or Erase[3] the Triple-DES System Master Key is zeroized, rendering the encrypted ECDSA Private Key undecipherable. Each event also deletes the ECDSA keys from non-volatile memory.	No
ECDSA Public Key(s)	This Public ECDSA key using NIST P-256, P-384 or P-521 curves is the public component of a module's ECDSA Key pair. They reside in the Network Certificate and are used for authenticating connections with other encryptors.	Internal Electronic	Stored in non-volatile system memory.	Electronic	Plaintext within X.509 certificate signed by trusted CA	The certificate is deleted from non-volatile system memory on tamper or Erase[3] command from a Crypto Officer.	No
ECDH Ephemeral Private Key	A Private ECDH ephemeral key using NIST P-256, P-384 or P-521 curves is the secret component of the ECDH key agreement key pair. It is generated during the key agreement process and destroyed once the process is complete.	Internal	Stored in volatile system memory.	No	N/A	Exists in volatile memory during the key agreement process.	No
ECDH Ephemeral Public Key	This Public ECDH ephemeral key using NIST P-256, P-384 or P-521 curves is the public component of the ECDH key agreement key pair. It is generated during the key agreement process and destroyed once the process is complete.	Internal Electronic	Stored in volatile system memory.	Electronic	N/A	Exists in volatile memory during the key agreement process.	No
ECDHE Shared Secret	The ECDHE Shared Secret is used to derive the DEK in point to point sessions or the GEK in group sessions	Internal Electronic	Stored in volatile system memory.	Electronic	N/A	Exists in volatile memory during the key agreement process.	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	**Storage**	**Sourced**	**Format**		
Module Certificate(s)	A X.509 certificate is associated with a session in an operational environment. It is produced, upon request from the module, and signed by the Certificate Authority (CA) to establish root trust between encryptors. Once a certificate has been authenticated, Far-end encryptors use the signed RSA Public Key to wrap the initial session keys (KEKs) used to encrypt a session. Alternatively, far end encryptors use the signed ECDSA public key to authenticate messages sent during the ECDH key agreement process.	Internal Electronic	Stored, in the plaintext, in non-volatile system memory	Electronic	Plaintext signed by trusted CA	The certificate is deleted from non-volatile system memory on tamper or Erase[3] command from a Crypto Officer.	No
Authentication Password	Up to 30 unique Crypto Officers (Administrators, Supervisors) or Users (Operators, Upgraders) may be defined, with associated passwords, within the module. The CLI uses the Authentication Password to authenticate Crypto Officers and Users accessing the system via the Local Console. The remote management application requires an authentication password that is used to uniquely authenticate each command to the module.	Internal Electronic	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 system memory	No	N/A	On tamper or Erase[3] the Triple-DES System Master Key is zeroized, rendering the encrypted Passwords undecipherable. Each event also deletes the User Table including passwords from non-volatile system memory	No
Key Encrypting Key	For each RSA based session (CI), the module generates an AES KEK using the NIST SP800-90A DRBG]. RSA-OAEP-256 key transport is used to transfer this key to a far-end module. The KEK persists for the life of the session and is used to secure the DEK that may be changed periodically during the session.	Internal Electronic	KEK is stored in plaintext, in volatile SDRAM system memory	Yes	Wrapped for transport using the far-end module's public RSA key	Zeroized at the end of a session, on tamper or Erase[3] and when power is removed from unit	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	Storage	Sourced	Format		
Data Encrypting Key	For each session (CI), the module also generates DEKs for each data flow path in the secure connection (one for the Initiator-Responder path and another for the Responder-Initiator path) using the NIST SP800-90A DRBG. For secure connections assigned to RSA certificates RSA-OAEP-256 key transport is used to transfer the initial DEK to a far-end module. Subsequent DEKs are transferred using AES key wrapping authenticated with HMAC-256. For each ECDSA/ECDH based connection (CI) a pair of encryptors use ECDH ephemeral key agreement to establish DEKs. These keys 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.	Internal Electronic	DEK is stored in plaintext, in volatile SDRAM system memory	Yes	RSA connections initially exchanged via RSA key transport and subsequently encrypted using KEK. ECDSA connections exchanged via ECDH ephemeral key agreement.	Zeroized at the end of a session, on tamper or Erase[3] and when power is removed from unit	No
Group Establishment Key (GEK)	When a slave joins an ECDSA/ECDH VLAN or multicast group session the key master from the group and the slave use ECDH ephemeral key agreement to establish a symmetric GEK used to wrap the group KEKs and DEKs using AES-256 authenticated with HMAC-256.	Internal Electronic	Stored in volatile system memory.	Electronic	N/A	Exists in volatile memory during the key agreement process.	No
SME HMAC keys	The SME HMAC keys are used to protect the integrity of the AES key wrap messages between encryptors	Internal	Stored in plaintext, in volatile system memory	No	N/A	Zeroized at the end of a session, on tamper or Erase[3] and when power is removed from unit	No
SNMPv3 Privacy Keys	For each SNMPv3 remote management session, the module uses an AES privacy key established during the Diffie-Hellman key agreement process to secure the control / flow path in the secure connection.	Internal Electronic	All SNMPv3 privacy keys are stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote management session and when power is removed from unit. Note Erase[3], reboot and tamper will end a remote session	No
DRBG Seed	Used for SP800-90 Hash_DRBG the 440 bit seed (initial V or state) value internally generated from nonce along with entropy input. A hardware based non-deterministic RNG is used for seeding the approved NIST SP 800-90A DRBG.	Internal	Stored in plaintext in volatile SDRAM system memory	Never exits the module	N/A	Destroyed after each Hash_DRBG random data request and when power is removed from unit or rebooted	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	Storage	Sourced	Format		
DRBG V Value	Used for SP800-90 Hash_DRBG, V is the Internal Hash_DRBG state value.	Internal	Stored in plaintext in volatile SDRAM system memory	Never exits the module	N/A	Destroyed after each Hash_DRBG random data request and when power is removed from unit or rebooted	No
DRBG Entropy Input and Nonce	Used for SP800-90 Hash_DRBG as input to the instantiate function.	Internal	Stored in plaintext in volatile SDRAM system memory	Never exits the module	N/A	Destroyed after each Hash_DRBG random data request and when power is removed from unit or rebooted	No
SNMPv3 Diffie Hellman Private Keys	A private Diffie-Hellman key is the secret component of the SNMPv3 Diffie-Hellman key pair. The key is created using Oakley group 14 for each remote SNMPv3 management session to enable agreement of the SNMPv3 privacy key between the module and the management station.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote management session and when power is removed from unit Note: Erase[3], reboot and tamper will end a remote session	No
SNMPv3 Diffie Hellman Public Keys	A public Diffie-Hellman key is the public component of the SNMPv3 Diffie-Hellman key pair. The key is created using Oakley group 14 for each SNMPv3 remote SNMPv3 management session to enable agreement of the SNMPv3 privacy key between the module and the management station.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote management session and when power is removed from unit Note: Erase[3], reboot and tamper will end a remote session	No
Remote CLI (SSH) Public Key	The Remote CLI Public Key is the public component of the RSA (2048 or 4096 bits) or ECDSA (NIST P-256, P-384 or P-521 curves) SSH key pair used to authenticate the remote client with the module.	External	Stored in non-volatile system memory.	Electronic	Plaintext	Deleted from non-volatile system memory on tamper or Erase[3] command from a Crypto Officer or when the record is deleted from table.	No
Remote CLI (SSH) Key Exchange Private Keys	A private Diffie-Hellman key (minimum size 2048 bits) or ECDH key (using NIST P-256, P-384 or P-521 curves) is the secret component of the Remote CLI (SSH) Key Exchange key pair. The key is created for each remote CLI session to enable agreement of the remote CLI privacy key between the module and the remote client.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote CLI session and when power is removed from unit Note: Erase[3], reboot and tamper will end a remote session	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	Storage	Sourced	Format		
Remote CLI (SSH) Key Exchange Public Keys	A public Diffie-Hellman key (minimum size 2048 bits) or ECDH key (using NIST P-256, P-384 or P-521 curves) is the public component of the Remote CLI (SSH) Key Exchange key pair. The key is created for each remote CLI session to enable agreement of the remote CLI privacy keys between the module and the remote client.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote CLI session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No
Remote CLI (SSH) HMAC keys	The remote CLI (SSH) HMAC keys are used to protect the integrity of the data transmitted across the secure SSH connection.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote CLI session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No
Remote CLI (SSH) Privacy Keys	For each remote CLI session, the module uses an AES privacy key established during the Diffie-Hellman or ECDH key agreement process to secure the control / flow path in the secure SSH connection.	Internal Electronic	All privacy keys are stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a remote management session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
SFTP (SSH) Private Key	The SFTP Private Key is the private component of the RSA (minimum modulus 2048 bits) or ECDSA (NIST P-256, P-384 or P-521 curves) SSH key pair used to authenticate the module with the remote server.	Internal Electronic	3-key Triple-DES-encrypted format, non-volatile system memory.	No	N/A	On tamper or Erase[3.] the Triple-DES System Master Key is zeroized, rendering the encrypted SFTP (SSH) Private Key undecipherable.	No
SFTP (SSH) Public Key	The SFTP Public Key is the public component of the RSA (minimum modulus 2048 bits) or ECDSA (NIST P-256, P-384 or P-521 curves) SSH key pair used to authenticate the module with the remote server.	Internal Electronic	Stored in non-volatile system memory.	Electronic	Plaintext	The key is deleted from non-volatile system memory on tamper or Erase[3.] Command from a Crypto Officer.	No
SFTP (SSH) Key Exchange Private Keys	A private Diffie-Hellman key (minimum size 2048 bits) or ECDH key (using NIST P-256, P-384 or P-521 curves) is the secret component of the SFTP (SSH) Key Exchange key pair. The key is created for each SFTP session to enable agreement of the SFTP privacy key between the module and the remote server.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an SFTP session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	**Storage**	**Sourced**	**Format**		
SFTP (SSH) Key Exchange Public Keys	A public Diffie-Hellman key (minimum size 2048 bits) or ECDH key (using NIST P-256, P-384 or P-521 curves) is the public component of the SFTP (SSH) Key Exchange key pair. The key is created for each SFTP session to enable agreement of the SFTP privacy keys between the module and the remote server.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an SFTP session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No
SFTP (SSH) HMAC keys	The SFTP (SSH) HMAC keys are used to protect the integrity of the data transmitted across the secure SSH connection.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an SFTP session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
SFTP (SSH) Shared Secret	The SFTP (SSH) Shared Secret is used to derive the SFTP (SSH) privacy keys	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an SFTP session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
SFTP (SSH) Privacy Keys	For each SFTP session, the module uses an AES privacy key established during the Diffie-Hellman or ECDH key agreement process to secure the control / flow path in the secure SSH connection.	Internal Electronic	All privacy keys are stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an SFTP session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
FTPS (TLS) Private Key	The FTPS (TLS) Private Key is the private component of the ECDSA ((using NIST P-256, P-384 or P-521 curves) FTPS key pair used to authenticate the module with the remote server.	Internal Electronic	3-key Triple-DES-encrypted format, non-volatile system memory.	No	N/A	On tamper or Erase[3.] the Triple-DES System Master Key is zeroized, rendering the encrypted FTPS (TLS) Private Key undecipherable.	No
FTPS (TLS) Public Key	The FTPS (TLS) Public Key is the public component of the ECDSA (using NIST P-256, P-384 or P-521 curves) FTPS key pair used to authenticate the module with the remote server.	Internal Electronic	Stored in non-volatile system memory.	Electronic	Plaintext within X.509 certificate self signed by the ftp server or a trusted CA	The certificate is deleted from non-volatile system memory on tamper or Erase[3.] command from a Crypto Officer	No

Key/CSP	Key Type and Use	Key/CSP Entry		Key/CSP Output		Key/CSP Destruction	Key/CSP Archiving
		Origin	**Storage**	**Sourced**	**Format**		
FTPS (TLS) Key Exchange Private Keys	A private ECDH key (using NIST P-256, P-384 or P-521 curves) is the secret component of the FTPS (SSH) Key Exchange key pair. The key is created for each FTPS session to enable agreement of the FTPS privacy key between the module and the remote server.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an FTPS session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No
FTPS (TLS) Key Exchange Public Keys	A public ECDH key (using NIST P-256, P-384 or P-521 curves) is the public component of the FTPS (SSH) Key Exchange key pair. The key is created for each FTPS session to enable agreement of the FTPS privacy keys between the module and the remote server.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an FTPS session and when power is removed from unit Note: Erase[3.], reboot and tamper will end a remote session	No
FTPS (TLS) HMAC keys	The FTPS (TLS) HMAC keys are used to protect the integrity of the data transmitted across the secure TLS connection.	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of a FTPS session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
FTPS (TLS) Master Secret	The FTPS (TLS) Master Secret is used to derive the FTPS (TLS) privacy keys	Internal	Stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an FTPS session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
FTPS (TLS) Privacy Keys	For each FTPS session, the module uses an AES privacy key established using ECDH to secure the control / flow path in the secure TLS connection.	Internal Electronic	All privacy keys are stored in plaintext, in volatile system memory	No	N/A	Destroyed at the end of an FTPS session and when power is removed from unit. Note Erase[3.], reboot and tamper will end a remote session	No
Firmware Upgrade RSA Public Keys	This Firmware Upgrade RSA Public 2048 bit key is the public component of a module's firmware upgrade RSA Key pair. It is used for authenticating the firmware upgrade image (signature verification only). The Firmware Upgrade RSA Public Key is embedded in the module's firmware.	External Electronic	Stored in non-volatile system memory.	Electronic	Plaintext	Key is embedded in the firmware and is not erased.	No

Note 1: While the certificates, maintained within the module, are listed as CSPs, they contain only public information.
Note 2: As per SP 800-133, all random data including cryptographic Key material is sourced unmodified from the NIST SP800-90A DRBG as required.
Note 3: Switching modes, selecting the front panel key press Erase sequence or pressing the concealed Emergency Erase button initiates a module Erase resulting in the destruction of this Key/CSP.

Note 4: The ECDH key agreement methodology as implemented in the module provides between 128 and 256 bits of encryption strength.
Note 5: The services above which utilize key establishment methods, shall be configured to use only the cipher suites labelled as "approved" when operating in the approved mode. Failure to utilize the approved cipher suites as per 0 and Table 19 of this security policy, will place the modules into a non-approved mode of operation.
Note 6: Triple-DES and the SMK are only used to encrypt CSPs within the module. The SMK is generated internally and is never transmitted from the module. As per SP 800-67rev2, a counter is employed to monitor Triple-DES 64 bit block encryption operations. If the counter reaches 2^{20} the SMK and all CSPs will be erased and the module will reboot. This is considered a safeguard operation and it is not expected to occur in the lifetime of the module.
Note 7: The System Master Key is never used for key wrapping for transporting keys.

6.2 Key and CSP zeroization

Zeroization of cryptographic Keys and CSPs is a critical module function that can be initiated by a Crypto Officer or under defined conditions, carried out automatically. Zeroization is achieved using the "Zeroization sequence" defined in section 6.2.1 below.

Crypto Officer initiated zeroization will occur immediately when the:

1. Module Erase command issued from the CLI or remote management application
2. Front Panel key press Erase sequence is selected
3. Concealed front panel Emergency Erase button is depressed

Automatic zeroization will occur immediately when the module is:

1. Switched from an Approved to non-Approved mode of operation
2. Switched from an non-Approved to Approved mode of operation
3. Physically tampered

The following sections describe the specific events that occur when zeroization initiated. Note zeroization behaviour is the same whether the module is configured to run in FIPS-Approved or non-Approved mode.

6.2.1 Zeroization sequence

Once initiated the module Zeroization sequence immediately carries out the following:

- Sets each session (CI) to DISCARD, before zeroizing the DEKs
- Zeroizes the System Master Key rendering the RSA and ECDSA Private Keys, User table (including authentication passwords) and other CSPs (Certificates, RSA keys) indecipherable
- Deletes all Certificate information
- Deletes RSA and ECDSA Private and Public keys, module Configuration and User table [1]
- Automatically REBOOTs the module destroying KEKs, Privacy and Diffie Hellman keys residing in volatile system memory

6.2.2 Erase command and key press sequence

A Crypto officer can initiate a module Erase remotely using the remote management application or when physically in the presence of the module using the management console CLI interface or front panel Erase key press sequence.

Zeroization of the module Keys and CSPs and is achieved using the zeroization sequence as defined in section 6.2.1.

6.2.3 Approved mode of operation

Switching the module to and from the FIPS Approved mode of operation will automatically initiate a Zeroization sequence to as defined in section 6.2.1 above.

[1] The RSA and ECDSA Private and Public keys, Configuration details and User table are encrypted by the System Master Key which, during an Erase, is the first CSP to be zeroized. Deleting the aforementioned CSPs is deemed good practise.

6.2.4 Tamper initiated zeroization

Zeroization will be initiated immediately upon detection of a tamper event. The Tamper Circuit is active at all times; the specific tamper response differs slightly based on the module's power state. From a practical standpoint the effect on the Keys and CSPs is the same.

The tamper initiated zeroization process achieves the following:

1. Zeroization of the System Master Key (SMK) rendering the RSA and ECDSA Private Keys, User table and other CSPs indecipherable. Zeroization of the SMK occurs irrespective of the powered state of the module.
2. When powered on and the Tamper Circuit is triggered, the module will automatically:
    a. Set the encryption mode for each session (CI) to DISCARD ensuring no user data is output from the module,
    b. Log the tamper event to the Audit Log,
    c. Set the System, Secure and Alarm LEDs to flash RED on the front panel and herald the tamper event via the internal speaker,
    d. Initiate the Zeroization sequence zeroizing all Session Keys (DEKs) and CSPs in volatile system memory and non-volatile Configuration and User account data,
    e. REBOOT the module.
3. When powered off and the Tamper Circuit is triggered, there are no Session Keys (DEKs) or CSPs in system volatile memory to be zeroized however upon re-powering the module, the zeroised System Master Key will indicate that the system has been tampered. The module will:
    a. Log the tamper event to the Audit log,
    b. Initiate the Zeroization sequence,
    c. Continue to the BOOT, returning the module to the un-Activated factory default state.
4. When the BOOT sequence has completed the module will have:
    a. Generated a new System Master Key,
    b. Re-created the default administration account,
    c. Set the encryption mode to DISCARD,
    d. Entered the factory default state ready for Configuration (as described in Section 8.3 below).

6.2.5 Emergency Erase

The Emergency Erase feature is initiated when the concealed front panel Emergency Erase button is depressed and follows the behaviour defined in section 6.2.4 Tamper initiated zeroization above.

6.3 Data privacy

To ensure user data privacy the module prevents data output during system initialization. No data is output until the module is successfully authenticated (activated) 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 data plane cryptographic keys and CSPs; zeroization occurs when the tamper circuit is triggered. In addition, the system's underlying operational environment logically separates key management functions and CSP data from the data plane.

6.4 Cryptographic Algorithms

CN9000 Series Encryptors employ the following approved cryptographic algorithms. Table 13 lists approved embedded software algorithms that are common to the CN9000 Series. Table 14 lists approved firmware algorithms that are specific to the CN9100 and CN9120 hardware.

Table 13 FIPS Approved Algorithms – CN9000 Series Common Crypto Library

Algorithm Type	Algorithm	FIPS Validation Certificate	Target Model Notes
CN9000 Series Crypto Library			**CN9100 / CN9120**
Symmetric Key	**Triple-DES** TCFB8[5] (e/d; KO 1)	Triple-DES #2427	
	AES CFB128 (e/d; 128,256)	AES #4556	
	AES CBC (e/d; 128,256)	AES #4556	
	AES CTR (int only; 128, 256)	AES #4556	
	AES ECB (e/d; 128, 256)	AES #4556	
Asymmetric Key	**RSA** Key(gen) (MOD: 2048) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); 2048; SIG(ver); 1024[4], 2048, 4096, SHS: SHA-1[2.], SHA-256	RSA #2483	
	ECDSA FIPS186-4: PKG: P-256, P-384 and P521 curves PKV: P-256, P-384 and P521 curves SigGen P-256 (SHA-256), P-384 (SHA-384) and P521 (SHA-512) curves SigVer P-256 (SHA-256), P-384 (SHA-384) and P521 (SHA-512) curves	ECDSA #1111	
	ECDH NIST P-256, P-384 and P521 curves are supported. SHA-256 is used for key derivation in accordance with SP800-56A	KAS #126	
Hashing	SHA-1 (BYTE only) SHA-256 (BYTE only) SHA-384 (BYTE only) SHA-512 (BYTE only)	SHS #3734	

Algorithm Type	Algorithm		FIPS Validation Certificate	Target Model Notes
HMAC	HMAC-SHA-1 [3.] (Key Sizes Ranges Tested: KS<BS) HMAC-SHA-256 (Key Sizes Ranges Tested: KS<BS)		HMAC #3010	
DRBG	NIST SP800-90A Hash_Based DRBG: [Prediction Resistance Tested: Not Enabled (SHA-256)]		DRBG #1506	
CKG	SP800-133 – section 6.1	Asymmetric key generation using unmodified DRBG output	Vendor Affirmed	
	SP800-133 – section 7.1	Direct generation of symmetric key using unmodified DRBG output	Vendor Affirmed	
	SP800-133 – section 7.2	Distribution of generated symmetric key (see KTS)	Vendor Affirmed	
	SP800-133 – section 7.3	Symmetric keys generated using ECDH key agreement in accordance with SP 800-56A	Vendor Affirmed	
KTS	NIST SP800-56B RSA-OAEP-256 Key Transport[6]		Vendor Affirmed	
KW	AES #4556 key wrapping authenticated with HMAC-256 #3010		Vendor Affirmed	

Note 1: The module does not generate RSA keys < 2048 for use in X.509v3 certificates in accordance with NIST SP800-131A.

Note 2: The module does not support the use of SHA-1 for X.509v3 certificate digital signatures in line with SP800-131A.

Note 3: HMAC keys < 112 bits are non-compliant in line with SP800-131A. HMAC keys for SSL and TLS are a minimum of 160 bits.

Note 4: The Firmware Upgrade RSA Public 1024-bit key is only used for firmware load signature verification when firmware is downgraded to legacy firmware.

Note 5: Triple-DES and the SMK are only used to encrypt CSPs within the module. The SMK is generated internally and is never transmitted from the module. As per SP 800-67rev2, a counter is employed to monitor Triple-DES 64 bit block encryption operations. If the counter reaches 2^{20} the SMK and all CSPs will be erased and the module will reboot. This is considered a safeguard operation and it is not expected to occur in the lifetime of the module...

Note 6: Approved (Vendor Affirmed) RSA-OAEP-256 key transport as per NIST SP-800-56B using 2048 bit keys (112 bit equivalent strength) with OAEP padding using SHA-256 can be employed to establish the AES 128 or 256 bit symmetric keys used to secure connections between cryptographic modules.

Note 7: As per SP 800-133, all random data including cryptographic Key material is sourced unmodified from the NIST SP800-90A DRBG as required. The module generates a minimum of 256 bits of entropy for key generation.

Table 14 FIPS Approved Algorithms – CN9100 and CN9120 Firmware Algorithms

Algorithm Type	Algorithm	FIPS Validation Certificate	Target Model Notes
CN9100 Module - Ethernet			**Ethernet Model**
Symmetric Key	**AES** CTR (int only; 128, 256)	AES #4113	Line rate: 100 Gbps
	AES ECB (e only; 128, 256)	AES #4113	Model number /description: A9100B 100G Ethernet Encryptor
CN9120 Module - Ethernet			**Ethernet Model**
Symmetric Key	**AES** CTR (int only; 128, 256)	AES #4557	Line rate: 100 Gbps
	AES ECB (e only; 128, 256)	AES #4557	Model number /description: A9120B 100G Ethernet Encryptor

6.5 Key Derivation Functions

CN9000 Series Encryptors employ the following application-specific Key Derivation Functions (KDFs). Table 15 lists the KDFs.

Table 15 FIPS Approved KDF

KDF	Hash Algorithm	FIPS Validation Certificate	Target Model Notes
CN9000 Series Common Crypto Library			**CN9100 and CN9120**
SNMP Privacy and Authentication Key	SHA-1	CVL (Cert.#1238)	No parts of the SNMP protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP
TLS	MD5/SHA-1	CVL (Cert.#1238)	No parts of the TLS protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP
SSH	SHA-1 SHA-256 SHA-384 SHA-512	CVL (Cert.#1238)	No parts of the SSH protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP

6.6 Non Approved and Allowed Security Functions

Table 16 Non-Approved and Allowed Security Functions

Function
A non-approved, non-deterministic RNG (NDRNG) is used to seed the approved NIST SP 800-90A Hash_DRBG. The module generates a minimum of 256 bits of entropy for key generation.
MD5 is a non-approved algorithm but allowed for use in FIPS mode in the TLS 1.0 / 1.1 KDF according to IG 1.23, example 2a and SP 800-135r1, section 4.2.1. TLS uses HMAC-MD5 with HMAC-SHA1 for the pseudorandom function (PRF). The TLS 1.0 and 1.1 KDF is performed in the context of the TLS protocol. Refer to Table 13 for the SHA and HMAC FIPS Validation Certificates.

In addition to the FIPS approved algorithms, the CN9000 Series also includes the following allowed algorithms.

Table 17 Allowed Algorithms

Function	Use
RSA Key Wrapping	RSA key wrapping using 2048 bit keys (112 bit equivalent strength) can be employed to establish the AES 128 or 256 bit symmetric keys used to secure connections between cryptographic modules.
ECDH Ephemeral Key Agreement	It is possible to configure an encryptor to use ECDH ephemeral key agreement with NIST P-256 (128 bit equivalent strength), P-384 (192 bit equivalent strength) or NIST P-521 (256 bit equivalent strength) curves to establish AES 256 bit symmetric keys used to secure encrypted connections between cryptographic modules. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.
SNMPv3 Diffie-Hellman Key Agreement	Diffie-Hellman Key Agreement using 2048 bit Oakley Group 14 (112 bit equivalent strength) is employed to establish the AES 128 bit SNMPv3 privacy keys used to secure the management interface between the management application and the cryptographic module.
Remote CLI (SSH) Diffie-Hellman Key Agreement	Diffie-Hellman Key Agreement using 2048 bit Oakley Group 14 (112 bit equivalent strength) is employed to establish the AES 128 or 256 bit Remote CLI (SSH) privacy keys used to secure the CLI session between the module and the remote client.
Remote CLI (SSH) ECDH Key Agreement	It is possible to configure an encryptor to use ECDH ephemeral key agreement with NIST P-256 (128 bit equivalent strength), P-384 (192 bit equivalent strength) or NIST P-521 (256 bit equivalent strength) curves to establish AES 256 bit symmetric keys used to secure the CLI session between the module and the remote client. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.
SFTP (SSH) Diffie-Hellman Key Agreement	Diffie-Hellman Key Agreement using 2048 bit Oakley Group 14 (112 bit equivalent strength) is employed to establish the AES 128 or 256 bit SFTP (SSH) privacy keys used to secure SFTP sessions between the module and the remote server.
SFTP (SSH) ECDH Key Agreement	It is possible to configure an encryptor to use ECDH ephemeral key agreement with NIST P-256 (128 bit equivalent strength), P-384 (192 bit equivalent strength) or NIST P-521 (256 bit equivalent strength) curves to establish AES 256 bit symmetric keys used to secure SFTP connections between the module and the remote server. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.
FTPS (TLS) ECDH Key Agreement	It is possible to configure an encryptor to use ECDH ephemeral key agreement with NIST P-256 (128 bit equivalent strength), P-384 (192 bit equivalent strength) or NIST P-521 (256 bit equivalent strength) curves to establish AES 256 bit symmetric keys used to secure FTPS connections between the module and the remote server. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.

Table 18 TLS (version 1.0-1.2) for FTPS Cryptographic Algorithms

OpenSSL[2] Cipher Suite	Authentication	Key Exchange	Symmetric Encryption	Hash for HMAC
ECDHE-ECDSA-AES256-SHA384	ECDSA[3]	ECDH[3]	AES-256-CBC	SHA384
ECDHE-ECDSA-AES128-SHA256	ECDSA[3]	ECDH[3]	AES-128-CBC	SHA256
ECDHE-ECDSA-AES256-SHA	ECDSA[3]	ECDH[3]	AES-256-CBC	SHA1
ECDHE-ECDSA-AES128-SHA	ECDSA[3]	ECDH[3]	AES-128-CBC	SHA1

Note 1: OpenSSL version 1.0.1h
Note 2: Minimum HMAC key size is 160 bits
Note 3: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.
Note 4: TLS for FTPS is only used for firmware upgrade image transfer.

Table 19 SSH (for Remote CLI and SFTP) Cryptographic Algorithms

Algorithm Type	Algorithm
Authentication	ECDSA[1]
	RSA[2]
Key Exchange	ECDH[1]
	DH[3]
Symmetric Encryption	AES-256-CTR
	AES-128-CTR
Hash for HMAC[4]	SHA-1
	SHA-256
	SHA-512

Note 1: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.
Note 2: Minimum RSA key size allowed is 2048 bits.
Note 3: Minimum DH key size allowed is 2048 bits.
Note 4: Minimum HMAC key size is 160 bits

Note: Please refer to Table 21 in section 8.4 for details on non-Approved algorithms in non-Approved mode of operation.

7. Self Tests

CN9000 Series cryptographic modules perform 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. Upon entering an error state an operator can attempt to clear the state by restarting the module. If the state cannot be cleared the module must be returned to the manufacturer. Table 20 summarizes the module's self tests.

The design of the CN9000 Series cryptographic modules 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.

Upon successful completion of the self tests the module will allow access via the CLI and remote management tools. The LCD will display the set time and date as well as the time since successful reboot (self tests passed).

Table 20 Self Tests

Table Legend

Halt (Secure)	Behaviour: The module will enter a Secure shutdown state and Halt ("Secure Halt"). Thereby preventing the module being configured and passing any data over the Network data output interface. Recovery: Attempt to recover by power-cycle. If the Secure Halt condition persists the module cannot be recovered and must be returned to the factory.
Erase	Behaviour: The module will be Erased and reset to Factory Defaults. Recovery: Re-activate, certify and attempt to pass Network data.
Error/Alarm	Behaviour: Error/Alarm logged. System state unchanged Recovery: Observe carefully and re-attempt, if error persists check "User Guide"

Self Test	Description	Fault
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.CN9000 Series KATs are divided into two distinct modules which correspond to the common module listed in table 13 and firmware module listed in table 14.	
CN9000 Series Common Crypto Library	The following CN9000 Series Common Crypto Library algorithms are tested: AES128 encrypt, AES128 decrypt, AES256 encrypt, AES256 decrypt, Triple-DES192 encrypt, Triple-DES192 decrypt, SHA-1, SHA-256, SHA-384, SHA-512, HMAC-SHA-1, HMAC-SHA-256, RSA1024 encrypt, RSA1024 decrypt, RSA2048 encrypt, RSA2048 decrypt, RSA4096 encrypt, RSA4096 decrypt, RSA-OAEP-SHA256 2048 encrypt, RSA-OAEP-SHA256 2048 decrypt, ECDSA P-256, P-384, and P-521 (Sign and Verify and KAT), ECDH P-256, P-384, and P-521 (primitive KAT) and SP 800-90A DRBG.	Halt
	The AES firmware modules are tested at power-up.	
CN9100 100G Ethernet	AES CTR128 (e/d; 128, 256)	Halt
CN9120 100G Ethernet	AES CTR128 (e/d; 128, 256)	Halt

Self Test	Description	Fault
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. Upon any file error the system will enter a Secure shutdown state and Halt ("Secure Halt")	Halt
Bypass Test	CN9000 Series modules support alternating between Bypass, Discard and Encrypt modes (which can be seen from the management interface). The configuration files that control the bypass/discard and encrypt settings are integrity checked using a stored checksum (32 bit CRC). On power-up the module calculates a fresh checksum for all configuration files and compares each to the stored values. Upon a mismatch an error is flagged. The error condition will result in a recreation of the configuration file with the factory default settings. Factory default settings are to fail safe, setting policy to Discard. An audit message is entered to reflect the re-initialisation. Any user change (crypto officer) to or from encrypt, bypass or discard shall cause an audit log entry.	Erase
Critical Functions	**Performed at power-up**	
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 however it is advisable that the battery be replaced immediately. The battery is located in the removable fan tray and can be ordered from the module's supplier. Battery alarm indication is available to all user roles via the alarm mechanism.	Alarm
Real Time Clock / Tamper Memory	The Real Time Clock (RTC) oscillator is checked at start-up and the Tamper memory is examined for evidence of a Tamper Condition.	Halt
Conditional Tests	**Performed, as needed, during operation**	
Bypass Test	The module supports alternating between Bypass, Discard and Encrypt modes (which can be seen from the management interface). The configuration files that control the bypass/discard and encrypt settings are integrity checked using a stored checksum (32 bit CRC). Conditional bypass tests are enforced by checking the CRC during each process initialisation that memory maps specific configuration data. If the CRC is valid, the process continues execution with that data, otherwise a re-initialisation is executed to failsafe values. Once running, a process will update the relevant configuration data when required, recalculating and storing the new CRC value.	Erase
Pair-wise Consistency	RSA 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 on their purpose, at the time they are used. RSA wrapping keys are tested by an encrypt/decrypt pair-wise consistency test; signature keys are tested by a sign/verify pair-wise	Halt

Self Test	Description	Fault
	consistency test. ECDSA Public and Private keys are used for the calculation and verification of digital signatures. These keys are tested at the time they are used with a sign/verify pair-wise consistency test.	
Firmware Load	When a new firmware image file is generated by the vendor, the file is encrypted and then signed with the firmware upgrade RSA private key. When any firmware load is applied to the encryptor in the field, the module verifies the authenticity of the firmware image file using its copy of the firmware upgrade RSA public key. Only firmware loads with a valid and verified firmware upgrade RSA signature are accepted.	Error
CRNGT for the NDRNG and DRBG	The non-deterministic RNGs are continuously tested according to SP800-90B (section 4.4). The DRBG is continuously tested according to FIPS140-2 (section 4.9.2).	Halt

Crypto Officers can run the power-up self-test on demand by issuing a module reboot command. This may be accomplished via 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 CN9000 Series Encryptors 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 CN9000 Series 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 the remote management application.

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

Note: Non-FIPS mode of operation is provided for interoperability with legacy systems. The module's factory default state (prior to commissioning as outlined in section 8.3) for the FIPS configuration setting is Enabled. The CN9000 Series must be explicitly configured to operate in a non-FIPS approved mode.

The console command is:

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

```
CN9100> fips on
FIPS mode enabled
```

The Senetas CM7 remote management application screen for reporting the FIPS status is found on the User Management screen, in the Access tab under FIPS PUB 140-2 Mode.

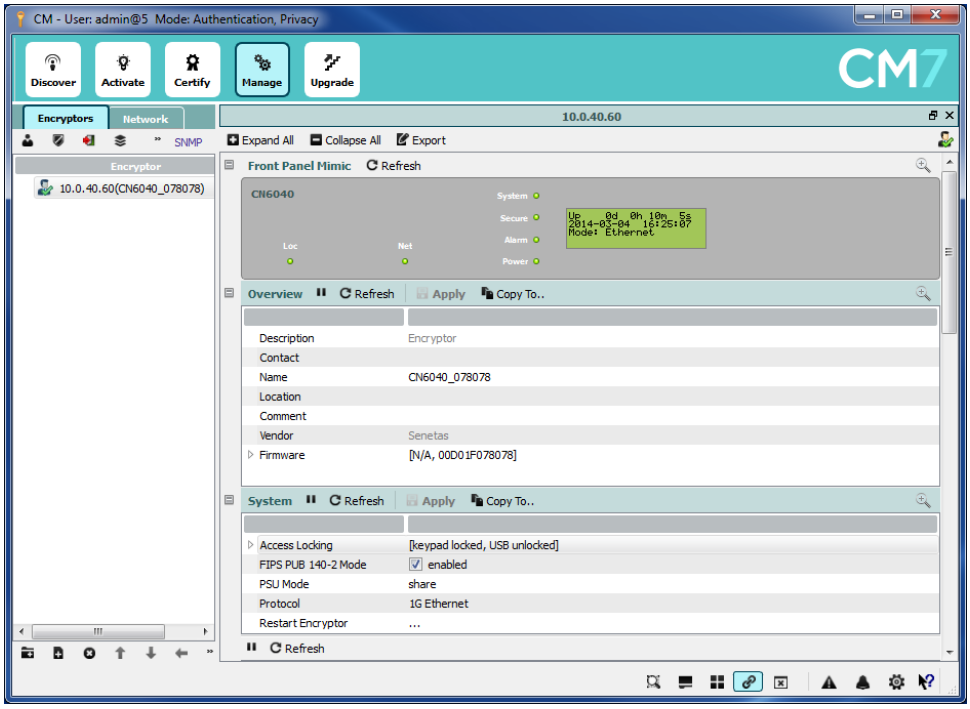

Figure 17 – FIPS Approved and non-Approved mode selection

Note: Read all of the instructions in this section before installing, configuring, and operating the CN9000 Series Encryptors.

8.1 Delivery

Before the shipment proceeds a serial number is allocated for the ordered module. Prior to the module shipping, a Shipping Advice form listing the purchase order number, the model number, the serial number and date of shipment is sent to the purchaser. When the module 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 Shipping Advice form, 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 the supplier should be informed immediately.

Upon receipt of a CN9000 Series 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 the CN9000 Series 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 front and rear 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 or switch, while the Network Interface will connect to the NTU provided by the network carrier.

8.3 Configuration – FIPS140-Approved mode

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 the remote management application to initialize the module and perform the configuration operations.

1. Power on the unit.

   The system boot-up sequence is entered each time the module is powered on and after a firmware restart. The CN9000 Series Encryptor 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 Secure shutdown state and Halt ("Secure Halt"). If this occurs the first time power is applied or any time in the future, the module will notify the CO that a persistent (hard) error has occurred and that the module must be returned for inspection and repair.

2. Follow the User Manual's **Commissioning** section to set the system's IP Address, Date and Time.

3. If the CM7 application is being run for the first time, it will ask if the CM7 installation will act as the Certification Authority (CA) for the secure network. If the user selects yes a private and public RSA or ECDSA key pair that will be used to sign X.509v3 Certificate Signing Requests from the module is generated by the CM7 application.

4. **Activate** the cryptographic module.

   A newly manufactured or erased cryptographic module must be **Activated** before X.509v3 certificate requests can be processed. See the User Manual's **Commissioning** section for details.

   Activation ensures that the default credentials of the 'admin' account are replaced with those specified by the customer prior to loading signed X.509v3 certificates in to the module.

   The updated user credentials (username and password) are transmitted to the encryptor using RSA 2048 public key encryption, and a hashing mechanism is used by the local administrator CO to authenticate the message.

5. Install a signed **X.509v3 certificate** into the cryptographic module.

   CN9000 Series Series cryptographic modules support X.509v3 Certificate Signing Requests (CSRs) and will accept certificates signed by the remote management application CM7 (when acting as a CA) as well as certificates signed by External CAs. In both cases each CN9000 Series cryptographic module supplies upon request an X.509v3 CSR containing the module's details and either a 2048 bit Public RSA key or an ECDSA Public key using NIST P-256, P-384 or P-521 curves.

   The administrator then takes the CSR and has it signed by either the trusted local CA (the remote management application CM7 for X.509v3 certificates using either a 2048 bit Public RSA key or an ECDSA Public key using NIST P-256, P-384 or P-521 curves) or an external CA for X.509v3 certificates using either a 2048 or 4096 bit Public RSA key or an ECDSA Public key using NIST P-256, P-384 or P-521 curves. For a typical deployment this procedure is repeated for all cryptographic modules in the network and the signed certificates are installed in to each module.

   After an X.509v3 certificate has been installed into CN9000 Series module the administrator can create supervisor and operator accounts.

   At this point the CN9000 Series Encryptor 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.

6. Ensure the encryptor is in FIPS 140-2 mode (default setting) via the Senetas CM7 remote management applications' **Management-Access** tab. See Figure 17 for details.

7. The maximum allowed number of encryptors in a multipoint group is 512. When operating in multipoint mode (MAC Multicast, VLAN or ISID mode) with Sender ID (SID) enabled the user must set a unique SID between 1 and 512 for each encryptor within the Multipoint group. Failure to do so will place the module in non-approved mode.

8. Configure the security policy to enable encrypted tunnels with other CN9000 Series modules.

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

8.4 Configuration - Non-Approved Mode

The CN9000 Series is capable of providing a number of non-approved services in order to support legacy functions such as SNMPv3 without privacy enabled and to provide remote AAA support, TACACS+ and other services.

These services are either gated via the FIPS enabled/disabled function or may be audited from the fips CLI command.

Configuring the CN9000 Series to and from FIPS mode of operation can be achieved using the CM7 remote management application or the local console via CLI. Once the change is affected the module will automatically erase and restart:

1. Navigate to the FIPS PUB 140-2 setting in **Management-Access** tab within the CM7 Application and *SET* the *Disable FIPS PUB 140-2 Mode* checkbox

   – OR -

2. Login via the front panel management console and execute the console command e.g. *"CN9100 Encryptor> fips off"*. See Figure 17 for details.

Table 21 Non-Approved Mode Services

Service	Description
Custom elliptic curve parameters	With FIPS mode disabled, users are able to load non-approved custom elliptic curve parameter sets for both CA and encryptor certificates for use by ECDSA and ECDH during secure session establishment. In this mode an extended list of OpenSSL[1] built in Elliptic Curves will also be available to the user.
RSA legacy certificate support	With FIPS mode disabled, users are able to load RSA certificates with key sizes < 2048 bits.
Entropy load	With FIPS mode disabled, users are able to load their own entropy pool onto the encryptor via the upgrade process. This entropy pool is used in place of the internal DRBG until it is exhausted or the service is disabled. The pool is deleted during an erase operation.
TACACS+[2]	TACACS+ can be configured in the module to allow AAA services to be provided from a remote TACACS+ server. When the user enables TACACS+ they are given a warning that TACACS+ uses non-approved algorithms and an audit log message stating that TACACS+ has been enabled is created. The fips CLI command will also give the user a warning if algorithms unsupported by FIPS140-2 are in service.

Note 1: OpenSSL version 1.0.1h
Note 2: TACACS+ uses MD5

Upon restart, the FIPS mode state can be checked using the remote management application or local console.

9. Mitigation of Other Attacks

This section is Not Applicable (N/A).