SENETAS
Security without compromise

Senetas Corporation Ltd., distributed by Thales SA (SafeNet)

CN Series Encryptors

FIPS 140-3 Non-Proprietary Security Policy
Level 3 Validation
September 2024

Module Name:	**CN Series Encryptors**	
Model Names:	**CN4010 1G Ethernet Encryptor** **CN4020 1G Ethernet Encryptor** **CN6010 1G Ethernet Encryptor** **CN6100 10G Ethernet Encryptor** **CN6110 1/10G Ethernet Encryptor** **CN6140 1/10G Multi Port Ethernet Encryptor** **CN9100 100G Ethernet Encryptor** **CN9120 100G Ethernet Encryptor**	
HW Versions:	**CN4000 Series:**	**A4010B (DC)** **A4020B (DC)**
	CN6000 Series:	**A6010B (AC), A6011B (DC), A6012B (AC/DC)** **A6100B (AC), A6101B (DC), A6102B (AC/DC)** **A6110B (AC), A6111B (DC), A6112B (AC/DC)** **A6140B (AC), A6141B (DC), A6142B (AC/DC)**
	CN9000 Series:	**A9100B (AC), A9101B (DC), A9102B (AC/DC)** **A9120B (AC), A9121B (DC), A9122B (AC/DC)**
FW Version:	**5.5.0**	

www.senetas.com

Document History

Authors	Date	Version	Comment
Senetas Corp. Ltd.	19-Dec-2023	1.00	CMVP Release for firmware version 5.5.0
Senetas Corp. Ltd.	11-Sep-2024	1.01	Interim validation update

Table of Contents

1. General

This is a non-proprietary FIPS 140-3 Security Policy for the Senetas Corporation Ltd. CN Series Encryptors (running firmware version 5.5.0) comprising of the CN4010, CN4020, CN6010, CN6100, CN6110, CN6140, CN9100 and CN9120 hardware cryptographic models. This Security Policy specifies the security rules under which the module operates to meet the FIPS 140-3 Level 3 requirements.

The CN Series Encryptors are distributed worldwide under different brands as depicted in this Security Policy. Senetas distributes under their own brand. Thales SA, the master worldwide distributor, distributes under the joint Thales/Senetas and SafeNet/Senetas brands (refer to Section 2.1.2).

FIPS 140-3 (Federal Information Processing Standards Publication 140-3), *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 twelve sections. For more information about the NIST/CCCS Cryptographic Module Validation Program (CMVP) and the FIPS 140-3 standard, visit www.nist.gov/cmvp.

This Security Policy, using the terminology contained in the FIPS 140-3 specification, describes how the CN Series models comply with the twelve sections of the standard. In this document, the CN4010, CN4020, CN6010, CN6100, CN6110, CN6140, CN9100 and CN9120 Encryptors are collectively referred to as the “CN Series” and individually as “the module” or “the encryptor”. The CN4010 and CN4020 models are collectively referred to as the “CN4000 Series”. The CN6010, CN6100, CN6110 and CN6140 models are collectively referred to as the “CN6000 Series”. The CN9100 and CN9120 models are collectively referred to as the “CN9000 Series”. The model name refers to all of the relevant module versions i.e. CN6010 refers to the module versions A6010B (AC), A6011B (DC), A6012B (AC/DC) (refer to Table 2 for a full listing).

This Security Policy and the associated CMVP certificate are for firmware version 5.5.0 only – the loading of any other firmware version on the specified CN Series Encryptors is out of scope of this FIPS 140-3 validation.

This Security Policy contains only non-proprietary information. Any other documentation associated with FIPS 140-3 conformance testing and validation is proprietary and confidential to Senetas Corporation Ltd. and is releasable only under appropriate non-disclosure agreements. For more information describing the CN Series systems, visit http://www.senetas.com.

1.1 References

For more information on the FIPS 140-3 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 140-3: Security Requirements for Cryptographic Modules.*

[2] *NIST Special Publication (SP) 800-140 FIPS 140-3 Derived Test Requirements (DTR).*

[3] *NIST Special Publication (SP) 800-140A CMVP Documentation Requirements.*

[4] *NIST Special Publication (SP) 800-140B CMVP Security Policy Requirements.*

[5] *NIST Special Publication (SP) 800-140Crev2 CMVP Approved Security Functions.*

[6] *NIST Special Publication (SP) 800-140Drev2 CMVP Approved Sensitive Security Parameter Generation and Establishment Methods.*

[7] *NIST Special Publication (SP) 800-140E CMVP Approved Authentication Mechanisms.*

[8] *NIST Special Publication (SP) 800-140Frev1 CMVP Approved Non-Invasive Attack Mitigation Test Metrics.*

[9] *ISO/IEC 19790:2012(E), Information technology — Security techniques — Security requirements for cryptographic modules.*

[10] *ISO/IEC 24759:2017(E), Information technology — Security techniques — Test requirements for cryptographic modules.*

[11] *NIST Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program.*

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

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

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

[15] *NIST Special Publication (SP) 800-131Arev2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*

[16] *NIST Special Publication (SP) 800-90Arev1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators.*

[17] *NIST Special Publication (SP) 800-56Arev3 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.*

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

[19] *NIST Special Publication (SP) 800-56Brev2, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography.*

[20] *NIST Special Publication (SP) 800-108rev1 Recommendation for Key Derivation Using Pseudorandom Functions.*

[21] *NIST Special Publication (SP) 800-56Crev2 Recommendation for Key-Derivation Methods in Key Establishment Schemes.*

[22] *NIST Special Publication (SP) 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation.*

[23] *NIST Special Publication (SP) 800-133rev2, Recommendation for Cryptographic Key Generation.*

[24] *NIST Special Publication (SP) 800-67rev2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.*

[25] *NIST Special Publication (SP) 800-135rev1, Recommendation for Existing Application-Specific Key Derivation Functions*

[26] *Senetas CN Series User Guides*

1.2 Acronyms and Abbreviations

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CFB	Cipher Feedback
CM7	Senetas Encryptor Remote Management Application Software
CI	Connection Identifier (used interchangeably with Tunnel)
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter Mode
DEK	Data Encrypting Key(s)
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESV	Entropy Source Validation
ESV (P)	Physical Entropy Source
ESV (NP)	Non-Physical Entropy Source
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FTPS	FTP Secure (FTP Over TLS)
Gbps	Gigabits per second
GCM	Galois Counter Mode
GDK	Group Derivation Key
HMAC	Keyed-Hash Message Authentication Code
IP	Internet Protocol
IV	Initialization Vector
KAS-ECC	Elliptic Curve Key Agreement Scheme (ECDH)
KAS-FCC	Finite Field Key Agreement Scheme (DH)
KAT	Known Answer Test
KDF	Key Derivation Function
KDK	Key Derivation Key

KEM	Key Encapsulation Method
KID	Key ID
KEK	Key Encrypting Key(s)
KMIP	Key Management Interoperability Protocol
KMS	Key Management Service
LED	Light Emitting Diode
MAC	Media Access Control (Ethernet source/destination address)
Mbps	Megabits per second
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OAEP	Optimal Asymmetric Encryption Padding
OQS	Open Quantum Safe
PKCS	Public Key Cryptography Standards
PSP	Public Security Parameter
PUB	Publication
QKD	Quantum Key Distribution
QRA	Quantum Resistant Algorithms
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
SFP	Small Form-factor Pluggable (transceiver)
SFTP	SSH File Transfer Protocol
SID	Sender ID
SMC	Gemalto’s Network Security Management Center
SME	Secure Message Exchange
SMK	System Master Key
SP	Special Publication
SPB	Shortest Path Bridging
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSP	Sensitive Security Parameter
TACACS+	Terminal Access Control Access Control Server
TIM	Transport Independent Mode
TLS	Transport Layer Security
TRANSEC	TRANsmission SECurity (also known as Traffic Flow Security or TFS)
X.509	Digital Certificate Standard RFC 2459

1.3 Security Levels

The module meets the overall Security Level 3 requirements for FIPS 140-3. See Table 1 below, which indicates the security level of each of the twelve sections of the FIPS 140-3 standard.

Table 1 Security Levels

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-tests	3
11	Life Cycle Assurance	3
12	Mitigation of Other Attacks	3

2. Cryptographic Module Specification

CN Series Encryptors are Hardware cryptographic modules. The CN6000 Series and CN9000 Series outer casing defines the cryptographic boundary aside from the pluggable transceivers, dual redundant power supplies and replaceable fan tray module that lie outside the cryptographic boundary. The CN4000 Series outer casing defines the cryptographic boundary aside from the pluggable transceivers on the CN4020 and the “AC to DC” plug-pack adapter which lie outside the cryptographic boundary. The cryptographic boundary is depicted by the red dashed line in Figure 1 below.

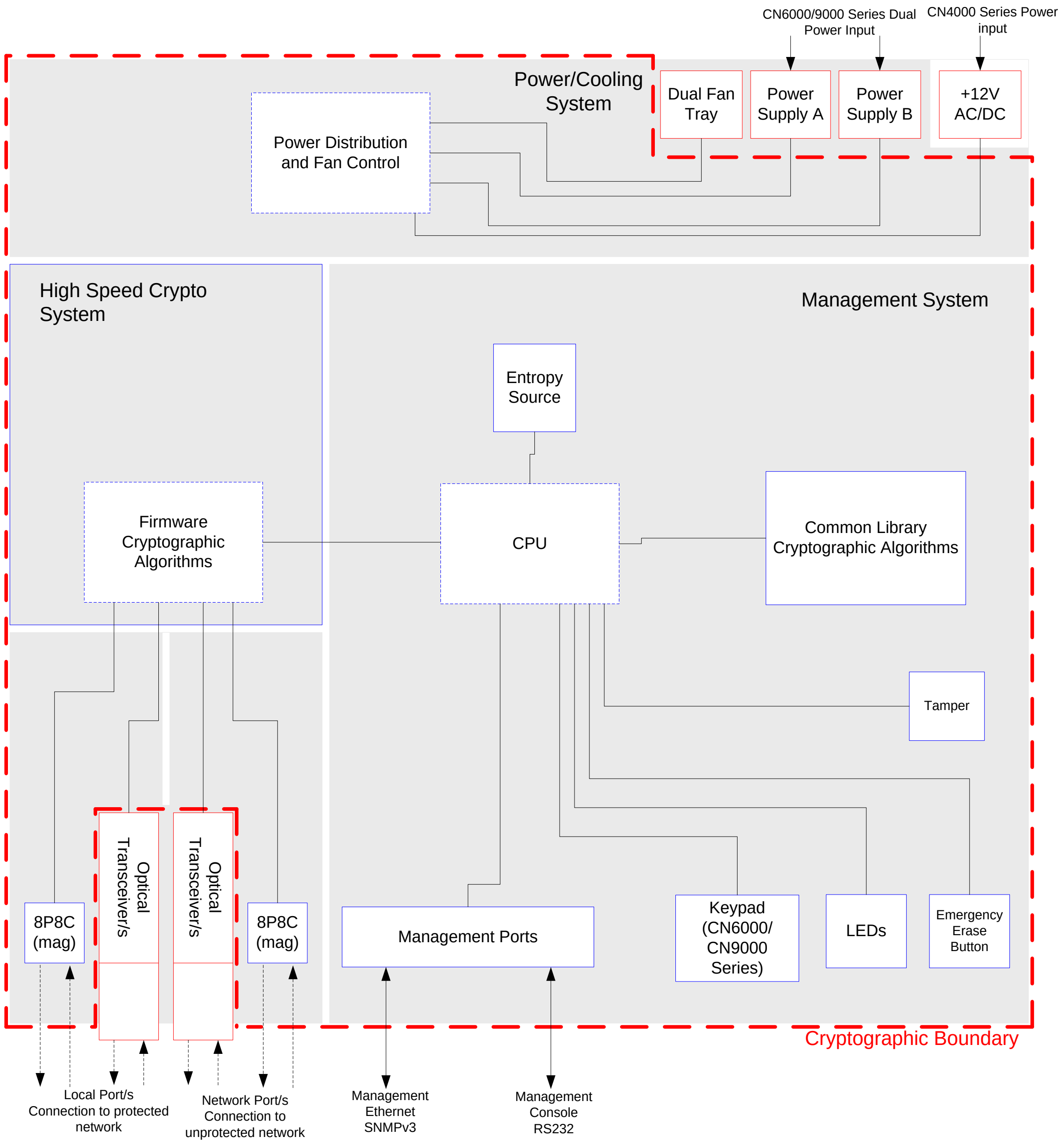

CN6000/9000 Series Dual Power Input
CN4000 Series Power input
Power/Cooling System
Power Distribution and Fan Control
Dual Fan Tray
Power Supply A
Power Supply B
+12V AC/DC
High Speed Crypto System
Management System
Entropy Source
Firmware Cryptographic Algorithms
CPU
Common Library Cryptographic Algorithms
Tamper
Optical Transceiver/s
Optical Transceiver/s
8P8C (mag)
8P8C (mag)
Management Ports
Keypad (CN6000/ CN9000 Series)
LEDs
Emergency Erase Button
Cryptographic Boundary
Local Port/s Connection to protected network
Network Port/s Connection to unprotected network
Management Ethernet SNMPv3
Management Console RS232

Figure 1 Cryptographic Boundary Block Diagram

2.1 Module Identification

CN Series Encryptors, with firmware version 5.5.0, provide data privacy and access control services for Ethernet networks. See model details summarized in Table 2.

Table 2 Cryptographic Module Tested Configuration

Model Name	Hardware Versions	Distinguishing Features			Firmware Version
		Power	Interface / Protocol	Transceiver/ Connector	
CN4010	A4010B [O][1,2] A4010B [Y][1,2] A4010B [T][1,2]	DC	1G Ethernet 1G TIM	RJ45	5.5.0
CN4020	A4020B [O][1,3] A4020B [Y][1,3] A4020B [T][1,3]	DC	1G Ethernet 1G TIM	SFP	5.5.0
CN6010	A6010B [O][1,4] A6010B [Y][1,4] A6010B [T][1,4]	AC	1G Ethernet 1G TIM	RJ45, SFP	5.5.0
	A6011B [O][1,4] A6011B [Y][1,4] A6011B [T][1,4]	DC			
	A6012B [O][1,4] A6012B [Y][1,4] A6012B [T][1,4]	AC/DC			
CN6100	A6100B [O][1,4] A6100B [Y][1,4] A6100B [T][1,4]	AC	10G Ethernet 10G TIM	XFP	5.5.0
	A6101B [O][1,4] A6101B [Y][1,4] A6101B [T][1,4]	DC			
	A6102B [O][1,4] A6102B [Y][1,4] A6102B [T][1,4]	AC/DC			
CN6110	A6110B [O][1,4] A6110B [Y][1,4] A6110B [T][1,4]	AC	1G Ethernet 1G TIM 10G Ethernet 10G TIM	RJ45, SFP+	5.5.0
	A6111B [O][1,4] A6111B [Y][1,4] A6111B [T][1,4]	DC			
	A6112B [O][1,4] A6112B [Y][1,4] A6112B [T][1,4]	AC/DC			
	A6140B [O][1,4] A6140B [Y][1,4] A6140B [T][1,4]	AC	1G Ethernet 1G TIM 10G Ethernet	SFP+	5.5.0

Model Name	Hardware Versions	Distinguishing Features			Firmware Version
		Power	Interface / Protocol	Transceiver/ Connector	
CN6140	A6141B [O][1,4] A6141B [Y][1,4] A6141B [T][1,4]	DC	10G TIM 4x10G Ethernet		
	A6142B [O][1,4] A6142B [Y][1,4] A6142B [T][1,4]	AC/DC			
CN9100	A9100B [O][1,5] A9100B [Y][1,5] A9100B [T][1,5]	AC	100G Ethernet	CFP4	5.5.0
	A9101B [O][1,5] A9101B [Y][1,5] A9101B [T][1,5]	DC			
	A9102B [O][1,5] A9102B [Y][1,5] A9102B [T][1,5]	AC/DC			
CN9120	A9120B [O][1,6] A9120B [Y][1,6] A9120B [T][1,6]	AC	100G Ethernet	QSFP28	5.5.0
	A9121B [O][1,6] A9121B [Y][1,6] A9121B [T][1,6]	DC			
	A9122B [O][1,6] A9122B [Y][1,6] A9122B [T][1,6]	AC/DC			

Note 1: Model variants distinguished by [O], [Y] and [T] 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
[T] Denotes Senetas Corp. Ltd. & Thales SA co-branded version

Note 2: These models derive their power from an “AC to DC” plug-pack adapter which is considered to be outside the cryptographic boundary.

Note 3: These models support pluggable SFP transceivers and derive their power from an “AC to DC” plug-pack adapter all of which are considered to be outside the cryptographic boundary.

Note 4: These models support pluggable SFP transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Note 5: This model supports pluggable CFP4 transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Note 6: This model supports pluggable QSFP28 transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

2.1.1 Module Images

CN4010 1G Ethernet Encryptor

CN4020 1G Ethernet Encryptor

CN6010 1G Ethernet Encryptor

CN6100 10G Ethernet Encryptor

CN6110 1/10G Ethernet Encryptor

CN6140 1/10G Multi Port Ethernet Encryptor

CN9100 100G Ethernet Encryptor

CN9120 100G Ethernet Encryptor

2.1.2 Branding

2.1.2.1 CN4010 & CN4020 branding

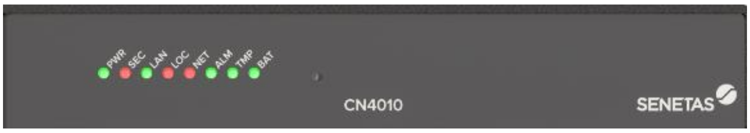
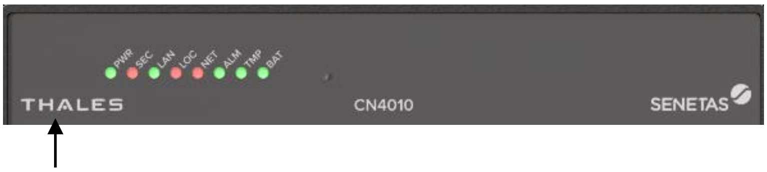
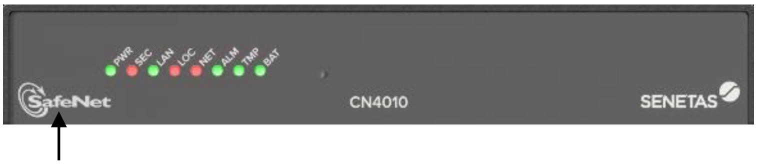


Figure 2 – Senetas sole-branding



Thales logo added to fascia

Figure 3 – Thales co-branding



SafeNet logo added to fascia

Figure 4 – SafeNet co-branding

2.1.2.2 CN6010, CN6100 & CN6110 branding

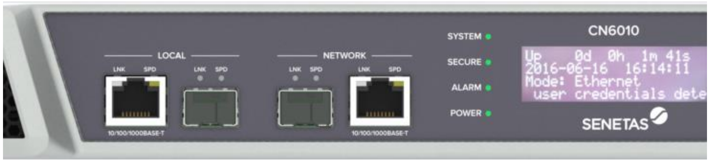


Figure 5 – Senetas sole-branding

Thales logo added to fascia

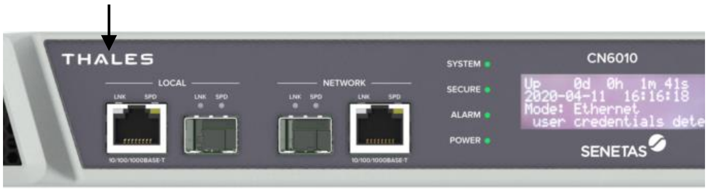


Figure 6 – Thales co-branding

SafeNet logo added to fascia

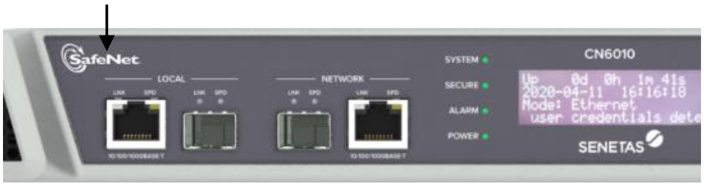


Figure 7 – SafeNet co-branding

2.1.2.3 CN6140, CN9100 & CN9120 branding

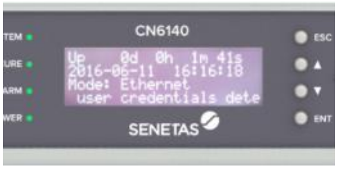
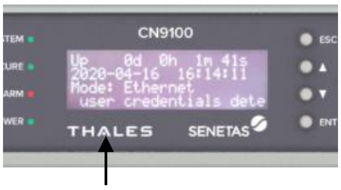
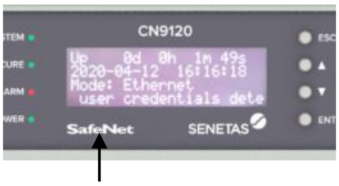


Figure 8 – Senetas sole-branding



Thales logo added to fascia

Figure 9 – Thales co-branding



SafeNet logo added to fascia

Figure 10 – SafeNet co-branding

2.2 Operational Overview

2.2.1 General

CN Series Encryptors operate in point-to-point and point-to-multipoint network topologies and at data rates ranging from 10Mb/s to 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 or CAT5/6 cables.

Securing a data link that connects two remote office sites is a common installation application.
Figure 11 provides an operational overview of two CN6010 encryptors positioned in the network.

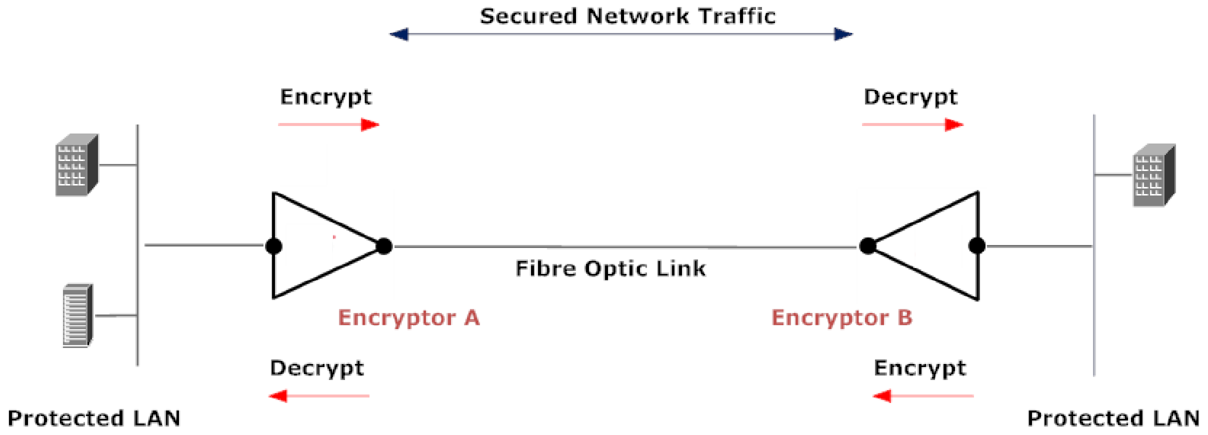


Figure 11 – CN6010 Operational Overview

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'.

CN 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 activated and `Certified` by a trusted body (refer to Section 2.3 for initial configuration steps) and exchange the key encrypting key (KEK) and initial data encryption key (DEK), using the RSA-OAEP-256 key transport process in accordance with SP 800-56Brev2 Section 9. Alternatively, ECDSA/ECDH utilises ephemeral key agreement for the purpose of establishing DEKs in accordance with SP 800-56Arev3. 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.

When deployed in layer 2 Ethernet networks, the modules can be configured in point-to-point mode (Line Mode) to establish connections between pairs of modules or they can be configured in multi-point mode (MAC Multipoint and VLAN modes) to establish connections between groups of encryptors. The authentication and key establishment algorithms in these modes of operation are determined by the X.509 certificate assigned to the connections.

Additionally, Transport Independent Mode[1] (TIM) allows concurrent secure connections between encryptors over OSI network layers 2, 3 and 4. DEKs are derived/distributed using one of two key provider mechanisms:

- Key Derivation Function (KDF)
- External Key Server using KMIP

When the KDF mechanism is configured the encryptors are loaded with a Key Derivation Key via CM7. The KDK is used to derive the DEKs using a KDF that conforms to SP 800-108rev1.

The external key server mechanism relies on a 3rd party Key Management Service (KMS) such as SafeNet's KeySecure to distribute the DEKs to the encryptors.

Figure 12 illustrates the conceptual data flow through a CN Series Encryptors.

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. Encryptor Sender ID (SID), MAC address or 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.

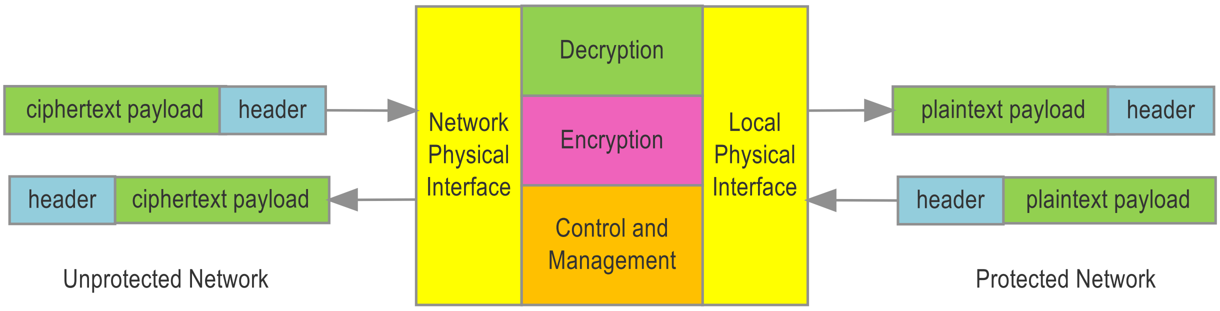


Figure 12 - Data Flow through the Encryptor

[1] TIM is not available on the CN9100 and CN9120 models, and the CN6140 model in 4x10G Mode.

2.2.2 Encryptor deployment

Figure 13 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 encryptors for each physical connection (link).

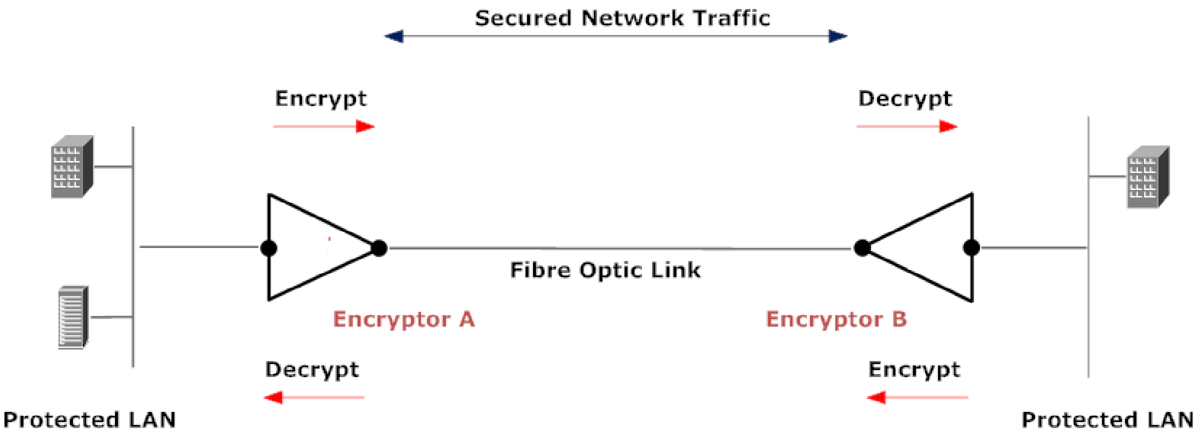


Figure 13 – Link (point-to-point) Configuration

Figure 14 illustrates a meshed network configuration. Each CN Series Encryptor is able to maintain simultaneous secured connections with many far end encryptors.

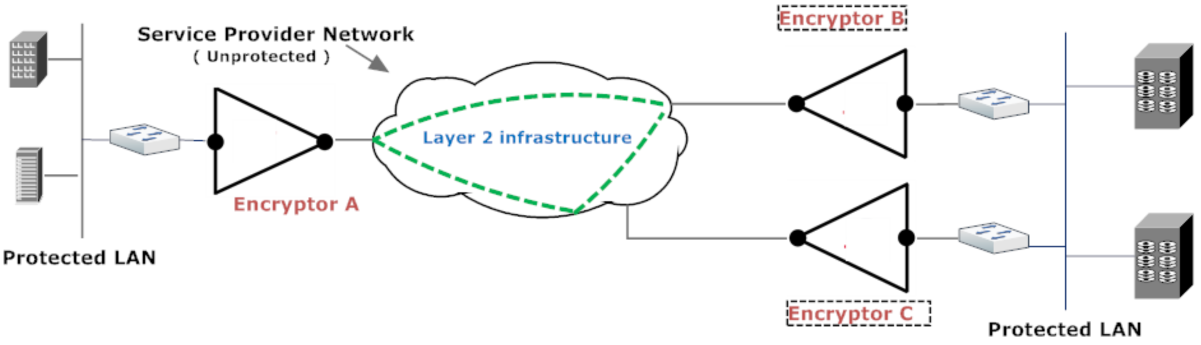


Figure 14 – Meshed (multipoint) Configuration

2.2.3 Encryptor management

Encryptors can be centrally controlled or managed across local and remote stations using the CM7 or SMC remote management applications. 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). When configuring remote CLI access the authentication algorithm is restricted to ECDSA. ECDSA keys are restricted to NIST P-256, P-384 and P-521 curves. Remote CLI access is disabled by default.

Approved mode of operation enforces the use of SNMPv3 privacy and authentication. Management messages are encrypted using AES-128 or AES-256.

2.3 Configuration

2.3.1 Administrator Guidance: Approved mode

Full configuration instructions are provided in the **User Guides [26]**. 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 140-3 approved mode.

When powering up the module for the first time, use the front panel or the CLI 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 CN 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 Guide’s [26] **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.509 certificate requests can be processed. See the User Guide’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.509 certificates into 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 to authenticate the message.

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

   CN 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 CN 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 into each module.

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

   At this point the CN Series Encryptor is able to encrypt in accordance with the configured security policy; the ENT (enter) key on the front panel is disabled; and the default factory account has been removed.

6. Ensure the encryptor is in FIPS 140-3 mode (default setting) via the Senetas CM7 remote management applications' **Management-Access** tab. See Figure 33 for details. Alternatively log into the CLI and run the CLI command "fips on" and follow the prompts. After the unit reboots log into the CLI and run the "fips" command without an argument. The command should return the message "FIPS mode enabled". Note: "fips mode" is enabled by default.

7. The maximum number of encryptors allowed in a multipoint group is 512. When operating in multipoint mode (MAC Multicast or VLAN mode) with Sender ID (SID) enabled, the user must set a unique SID between 1 and 512 for each encryptor within the Multipoint group.
8. Configure the security policy to enable encrypted tunnels with other CN Series modules.

   Configuration of the security policy is network specific; refer to the User Guide [26] for specific details.

Note: The module also supports TACACS+. If TACACS+ is enabled the module is no longer considered to be in approved mode.

2.3.2 non-Administrator Guidance

Non-administrators (Operator privilege level ref. **Table 13**) are able to view the modules configuration parameters and message logs. Non-administrators are not able to configure the module. Please refer to the **User Guides [26]** for comprehensive information on non-Administrator (Operator) functions.

2.4 Ethernet implementation

Basic operation

The Ethernet encryptor provides layer 2, 3 and 4 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 15 below.

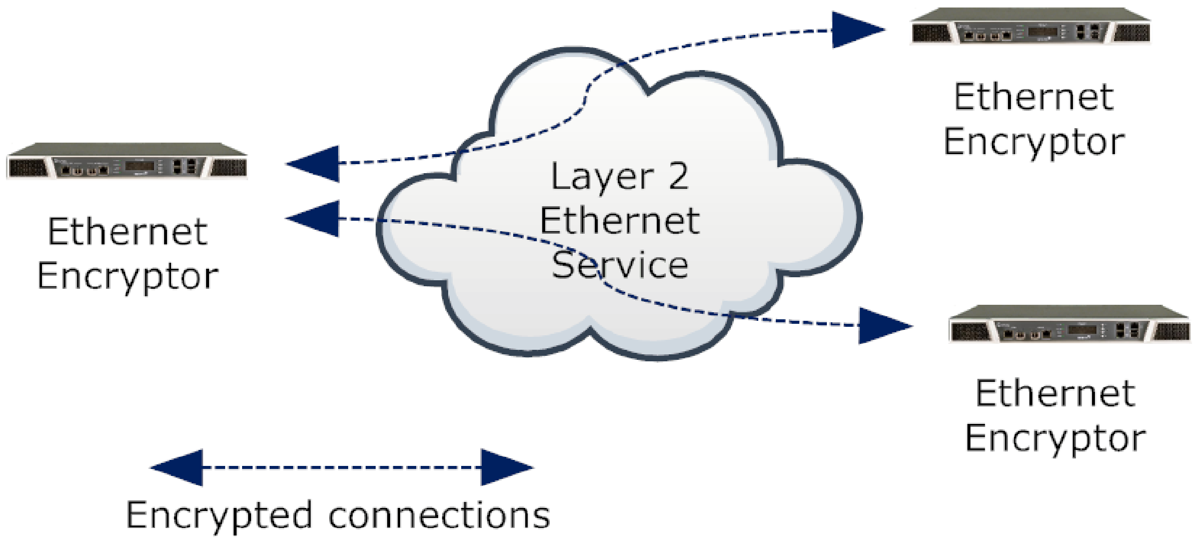


Figure 15 – Layer 2 Ethernet connections

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

CN Series tunnels are encrypted using CAVP validated AES algorithms. The CN4010, CN4020, CN6010, CN6110 (1G mode) and CN6140 (1G mode) 1G Ethernet encryptors support AES encryption with a key size of 128 or 256 bits in cipher feedback (CFB), counter (CTR) and Galois Counter (GCM) modes. The CN6100, CN6110 and CN6140 in 10G Ethernet mode and the CN9000 Series support AES encryption with a key size of 128 or 256 bits in counter (CTR) and Galois Counter (GCM) modes.

Connections between encryptors use a unique key pair with a separate key for each direction. Unicast traffic can be encrypted using AES CFB, CTR or GCM modes whereas Multicast/VLAN traffic in a meshed network must use AES CTR or GCM modes.

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.

2.4.1 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 MAC address or 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.

2.4.2 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.

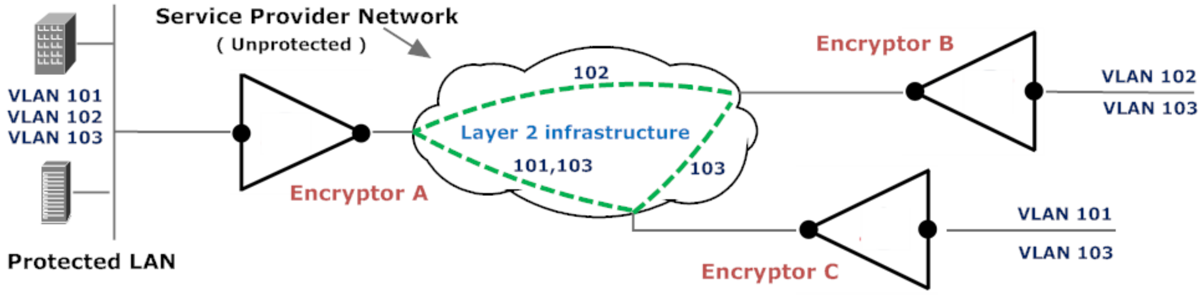


Figure 16 – Multipoint VLAN connections

2.4.3 Transport Independent Mode (TIM) operation

In Transport Independent Mode each encryptor in the network must be configured with a unique Sender ID (SID), The SID is sent in a shim inserted into each encrypted frame and is used by the receiving encryptor to identify the origin of the frame. When running in this mode, the SID is interchangeably referred to as the Key ID (KID).

Egress data flow (Encrypt data received on Local port and transmitted on Network Port)

Each encryptor has a single transmission 256-bit AES Data Encrypting Key (DEK) and all secure traffic is encrypted using that key.

Ingress data flow (Decrypt data received on Network port and transmitted on Local Port)

When an encryptor receives an encrypted frame, it uses the KID in the frame’s shim to identify the key to use for decryption. If the receiver doesn’t have keys for the received KID, it will request them from the configured key provider. A receiver must store two DEKs plus a salt for every peer encryptor that it communicates with.

TIM key updates

In Transport Independent Mode keys are periodically updated using either a time-based mechanism or a frame counter-based mechanism.

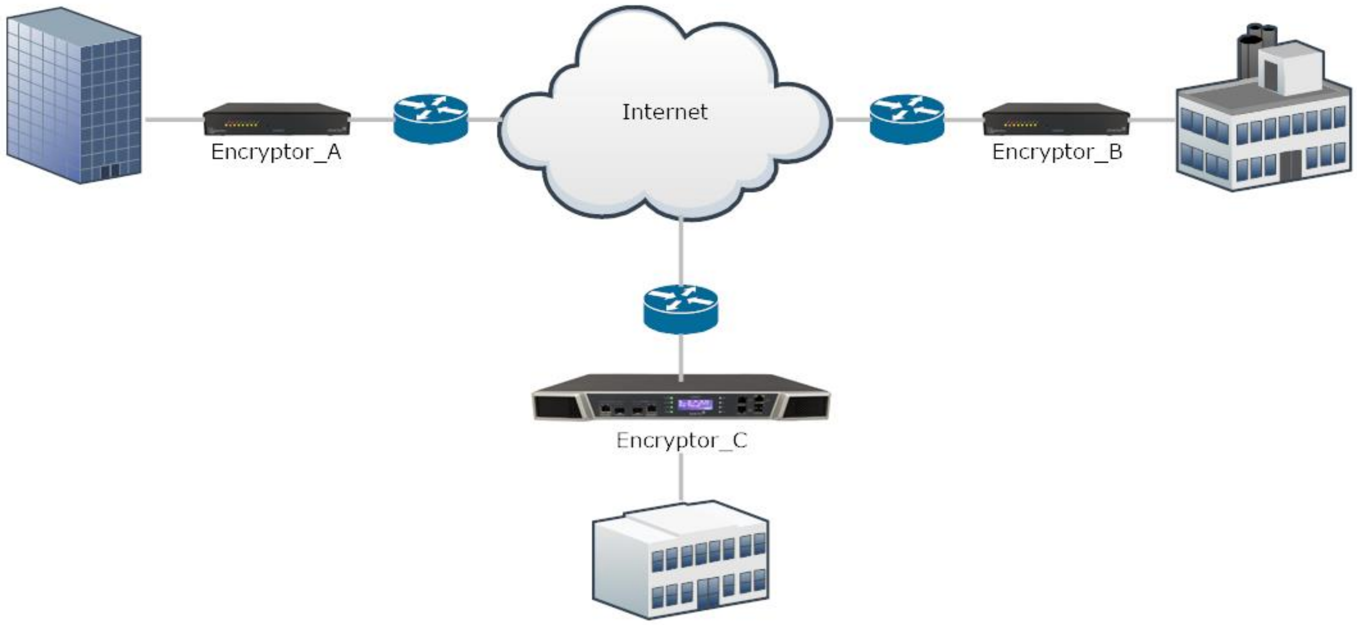


Figure 17 – Transport Independent Mode connections

2.5 Hybrid Session Establishment

Optionally, a hybrid mode for session establishment is available in line with NIST guidance for use of both approved and quantum resistant key establishment/derivation methods. When operating in this mode, the approved methods may be augmented with both Quantum Resistant Algorithm methods, and/or Quantum Key Distribution mechanisms.

2.5.1 Quantum Resistant Algorithms (QRA)

The CN Series Encryptors support the use of candidate Quantum Resistant Algorithms as available from the Open Quantum Safe initiative. The user can select from a full list consisting of the RSA/ECDSA algorithms and the new OQS signing algorithms. The keys established using the approved RSA/ECDH algorithms are combined with data established using the Quantum Resistant Algorithms.

2.5.2 Quantum Key Distribution (QKD)

The CN Series Encryptors support the use of Quantum Key Distribution devices such as ID Quantique’s Cerberis QKD system or any industry standard ETSI compliant QKD systems for hybrid key establishment. For hybrid key establishment the keys distributed using the approved RSA/ECDH algorithms are combined with the data derived from the QKD server.

2.6 TRANSEC operation

Traffic Analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. TRANSEC is TRANsmission SECurity and is used to disguise patterns in network traffic to prevent Traffic Analysis. TRANSEC mode can be optionally enabled between two end points of a point-point rate-limited layer 2 service provider network.

When operating in TRANSEC mode (CN4000 and CN6000 Series only) transport frames exit the network port at a constant rate irrespective of the rate at which user data arrives at local port. This ensures that Traffic Analysis, if performed, would generate no useful insight into the user data. The transport frame rate and length are user configurable. AES encryption protects the user data and when operating in GCM encryption mode provides the additional guarantee of data authentication.

TRANSEC mode coupled with AES-256 GCM provides triple layer protection of user data.

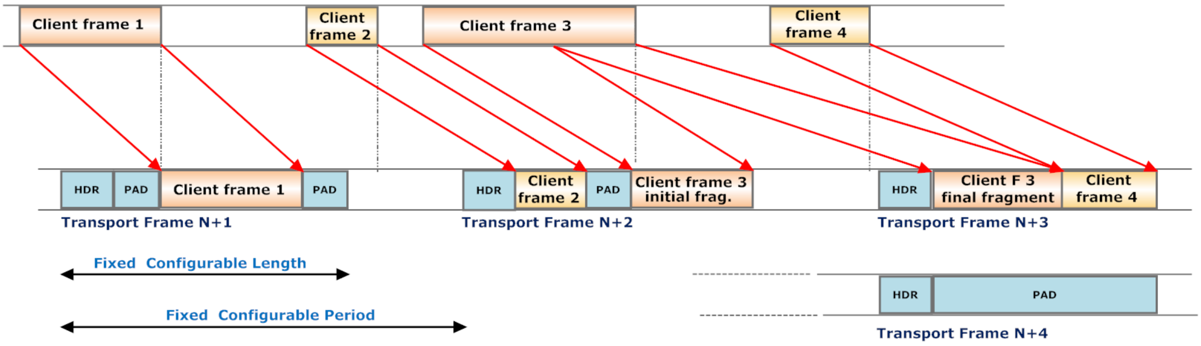


Figure 18 – TRANSEC constant rate transport frame assembly

2.7 Cryptographic Algorithms

2.7.1 Approved Algorithms

2.7.1.1 CN Series Common Crypto Library Algorithms

Table 3 lists approved software algorithms that are common to the CN Series Encryptors. These algorithms are used during the establishment of secure connections (SME), for management services (SNMPv3, TLS and SSH) and to generate and encrypt CSPs.

Table 3 Approved Algorithms – CN Series Common Crypto Library

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3451	Triple-DES SP 800-67rev2	TCFB8[1] (d; KO 1)	Three key (192 bits)	Decryption of CSPs after upgrade from legacy versions of code. CSPs are then encrypted using AES256
A3451	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[2] (e/d) CBC (e/d) GCM (e/d; Internal IV, AAD=0 to 256)	128-bit 256-bit	Symmetric Encryption/ Decryption
A3451	RSA FIPS186-4	KeyGen[3]; MOD: 2048 ALG[RSASSA-PKCS1_V1_5]: SigGen; MOD: 2048 SHS: SHA-256 SigVer; MOD: 2048 SHS: SHA-256, SHA-384 and SHA-512 SigVer; MOD: 4096 SHS: SHA-256, SHA-384 and SHA-512	2048-bit 4096-bit	Key Generation Signature Generation/ Verification
A3451	ECDSA FIPS186-4	KeyGen KeyVer SigGen SigVer	P-256 P-384 P-521	Key Generation Signature Generation/ Verification
A3451	KAS-ECC SP 800-56Arev3	Elliptic Curve Diffie-Hellman (Cofactor) Ephemeral Unified Model key agreement	NIST P-256, P-384 and P-521 curves[8] are supported and SHA-256, SHA-384 and SHA-512 (respectively) are	Key Establishment

			used for key derivation	
A3451	KAS-FFC SP 800-56Arev3	dhEphem key agreement	MODP-2048-bit Oakley Group 14[9] using SHA-256 for key derivation	Key Establishment
A3451	SHA FIPS 180-4	SHA-1[4] (BYTE only) SHA-256 (BYTE only) SHA-384 (BYTE only) SHA-512 (BYTE only)		Hashing
A3451	HMAC FIPS 198-1	HMAC-SHA-1[5] HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Key Sizes Ranges Tested: KS<BS	Keyed Hashing
A3451	DRBG SP 800-90Arev1	Hash_Based DRBG: [Prediction Resistance Tested: Not Enabled (SHA-256)]		Random Number Generation
A3451	KBKDF SP 800-108rev1	Counter based KDF using HMAC-SHA-256		Key Derivation
A3451	KTS-IFC SP 800-56Brev2	RSA-OAEP-256 Key Transport[6]		Key Transport
A3451	KTS FIPS 140-3 IG D.G	AES-256[7] CFB key wrapping authenticated with HMAC-SHA-256	256-bit	Key Transport/ Key Wrapping
A3451	SNMP KDF[10] (CVL) SP 800-135rev1	SHA-1 SHA-256		Key Derivation
A3451	TLS v1.2 KDF[11] (CVL) RFC5246 TLS v1.2 KDF[11] (CVL) RFC7627 SP 800-135rev1	SHA-256 SHA-384		Key Derivation
A3451	SSH KDF[12] (CVL) SP 800-135rev1	SHA-256 SHA-512		Key Derivation
E51	ESV (P)[13] SP 800-90B		256-bit	Entropy source for DRBG
E49	ESV (NP)[14] SP 800-90B		256-bit	Entropy source for DRBG
Vendor Affirmed	CKG SP 800-133rev2	Sections 5.1 & 5.2 - Asymmetric key generation using unmodified DRBG output		Key Generation
		Section 6.1 - Direct generation of symmetric key using unmodified DRBG output		Key Generation
		Section 6.2.1 - Symmetric keys generated using ECDH key agreement in accordance with SP 800-56Arev3 (see KAS-ECC)		Key Generation
		Section 6.4 - Distribution of generated symmetric key (see KTS)		Key Transport

Note 1: Triple-DES is only used to decrypt CSPs when upgrading from legacy versions of software. The CSPs are subsequently re-encrypted using AES-256 CFB. Triple-DES is no longer used by the module for encryption operations.

Note 2: AES-ECB Is only validated as part of the AES-CTR validation. The mode is not actively used by the module.

Note 3: The module does not generate RSA keys < 2048 for use in X.509v3 certificates in accordance with SP 800-131Arev2.

Note 4: The module does not support the use of SHA-1 for X.509v3 certificate digital signatures in line with SP 800-131Arev2.

Note 5: HMAC keys < 112 bits are non-compliant in line with SP 800-131Arev2. HMAC keys for SSL and TLS are a minimum of 160 bits.

Note 6: Approved RSA-OAEP-256 key transport as per SP 800-56Brev2 Section 9 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: AES-256 key wrapping provides 256 bits of encryption strength and can be employed to establish the AES 128- or 256-bit symmetric keys used to secure connections between cryptographic modules.

Note 8: 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. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.

Note 9: 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.

Note 10: No parts of the SNMP protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

Note 11: No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

Note 12: No parts of the SSH protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

Note 13: The CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120 models employ a physical entropy source.

Note 14: The CN6100 employs a non-physical entropy source

2.7.1.2 TLS AES-GCM Key and IV generation (refer to Table 3 above)

- The module conforms to TLSv1.2 GCM cipher suites as specified in SP 800-52rev2, Section 3.3.1.
- When the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key according to RFC 5246.
- In case the module’s power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established.

Table 4 Approved Algorithms – CN6100 ESV (NP) Conditioning Component

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3449	SHA-3 FIPS 202	SHA3-256 (BYTE only)		ESV Conditioning

Table 5 Approved Algorithms – CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120 ESV (P) Conditioning Component

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3450	SHA FIPS 180-4	SHA-256 (BYTE only)		ESV Conditioning
A3450	HMAC FIPS 198-1	HMAC-SHA-256	Key Sizes Ranges Tested: KS<BS	ESV Conditioning

2.7.1.3 CN Series Firmware Algorithms

Table 6 below lists approved firmware algorithms that are specific to the CN4010, CN4020, CN6010, CN6100, CN6110, CN6140, CN9100 and CN9120 hardware versions. These AES implementations are used to encrypt/decrypt data plane traffic.

Table 6 Approved Algorithms – CN Series Firmware Algorithms

CN4010 Module Version 1.10 – 1G Ethernet Mode				
CAVP Cert	**Algorithm and Standard**	**Mode/Method**	**Description/ Key Size(s)/ Key Strength(s)**	**Use/ Function**
A3435	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN4010 Module Version 1.10 – 1G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3436	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN4020 Module Version 1.10 – 1G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3437	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN4020 Module Version 1.10 – 1G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3438	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6010 Module Version 1.10 – 1G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3439	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6010 Module Version 1.10 – 1G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3440	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6100 Module Version 1.11 – 10G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3459	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6100 Module Version 1.11 – 10G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function

A3458	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV[2], AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6110 Module Version 1.10 – 1G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3549	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6110 Module Version 1.10 – 1G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3443	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6110 Module Version 1.11 – 10G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3441	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6110 Module Version 1.11 – 10G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3442	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6140 Module Version 1.10 – 1G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3445	AES FIPS PUB 197, SP 800-38A SP 800-38D	CFB128 (e/d) CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6140 Module Version 1.10 – 1G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3460	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6140 Module Version 1.11 – 10G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3448	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6140 Module Version 1.11 – 10G Ethernet TIM

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3444	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN6140 Module Version 1.11 – 4x10G Ethernet mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3492	AES FIPS PUB 197, SP 800-38A	CTR (e) ECB[1] (e)	128-bit 256-bit	Data Plane Encryption

CN9100 Module Version 1.3 – 100G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3446	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

CN9120 Module Version 1.3 – 100G Ethernet Mode

CAVP Cert	Algorithm and Standard	Mode/Method	Description/ Key Size(s)/ Key Strength(s)	Use/ Function
A3447	AES FIPS PUB 197, SP 800-38A SP 800-38D	CTR (e) ECB[1] (e) GCM (e/d; Internal IV, AAD=112 to 688)	128-bit 256-bit	Data Plane Encryption

Note 1: AES-ECB Is only validated as part of the AES-CTR validation. The mode is not actively used by the module.

2.7.1.4 AES-GCM Key and IV generation for data-plane encryption (refer to Table 6 above)

- The IV is 96 bits in length and is internally generated deterministically in compliance with Section 8.2.1 of SP 800-38D.

2.7.1.5 Cryptographic Protocol Algorithms

2.7.1.5.1 Secure Message Exchange (SME) protocol algorithms

The Senetas Secure Message Exchange (SME) protocol is used to establish secure connections between modules. The approved cryptographic algorithms employed by the SME protocol are listed in Table 7 below.

Table 7 SME Cryptographic Algorithms

Algorithm Type	Algorithm
Authentication	RSA[2] ECDSA[1]
Key Exchange	ECDH[1] RSA-OAEP AES-256-CFB
Hash for HMAC	SHA-256
ECDH KDF	SHA-256 SHA-384 SHA-512
AES Key Wrap key (KEK & GEK) and HMAC key KDF (KBKDF)	HMAC-SHA256
Signature	SHA-256 SHA-384 SHA-512
Symmetric Encryption	AES-128-CFB AES-256-CFB AES-128-CTR AES-256-CTR AES-128-GCM AES-256-GCM

Note 1: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.
Note 2: The module does not generate RSA keys < 2048 for use in X.509v3 certificates in accordance with SP 800-131Arev2.

2.7.1.5.2 TLS protocol algorithms

The TLS protocol (version 1.2) is used for FTPS (firmware upgrades), RESTful interface and KMS (KeySecure). The approved cryptographic algorithms employed by the TLS protocol are listed in Table 8 and Table 9 below.

Table 8 TLS Cryptographic Algorithms (FTPS, RESTful)

OpenSSL[1] Cipher Suite	Authentication	Key Exchange	Symmetric Encryption	Hash for HMAC[2]
ECDHE-ECDSA-AES256-GCM-SHA384	ECDSA[3]	ECDH[3]	AES-256-GCM[4]	SHA-384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDSA[3]	ECDH[3]	AES-128-GCM[4]	SHA-256
ECDHE-ECDSA-AES256-SHA-384	ECDSA[3]	ECDH[3]	AES-256-CBC	SHA-384
ECDHE-ECDSA-AES128-SHA-256	ECDSA[3]	ECDH[3]	AES-128-CBC	SHA-256

Note 1: OpenSSL version 1.1.1n.
Note 2: Minimum HMAC key size is 256 bits.
Note 3: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.
Note 4: The AES GCM IV is internally generated randomly in compliance with TLS 1.2 GCM Cipher Suites for TLS and Section 8.2.2 of SP 800-38D.

Table 9 TLS Cryptographic Algorithms (KMS)

OpenSSL[1] Cipher Suite	Authentication	Key Exchange	Symmetric Encryption	Hash for HMAC[2]
ECDHE-ECDSA-AES256-GCM-SHA384	ECDSA[3]	ECDH[3]	AES-256-GCM[4]	SHA-384
ECDHE-ECDSA-AES128-GCM-SHA256	ECDSA[3]	ECDH[3]	AES-128-GCM[4]	SHA-256
ECDHE-ECDSA-AES256-SHA-384	ECDSA[3]	ECDH[3]	AES-256-CBC	SHA-384
ECDHE-ECDSA-AES128-SHA-256	ECDSA[3]	ECDH[3]	AES-128-CBC	SHA-256
ECDHE-RSA-AES256-GCM-SHA384	RSA[5]	ECDH[3]	AES-256-GCM[4]	SHA-384
ECDHE-RSA-AES128-GCM-SHA256	RSA[5]	ECDH[3]	AES-128-GCM[4]	SHA-256
ECDHE-RSA-AES256-SHA-384	RSA[5]	ECDH[3]	AES-256-CBC	SHA-384
ECDHE-RSA-AES128-SHA-256	RSA[5]	ECDH[3]	AES-128-CBC	SHA-256

Note 1: OpenSSL version 1.1.1n.
Note 2: Minimum HMAC key size is 256 bits.
Note 3: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.
Note 4: The AES GCM IV is internally generated randomly in compliance with TLS 1.2 GCM Cipher Suites for TLS and Section 8.2.2 of SP 800-38D.
Note 5: Minimum RSA key size allowed is 2048 bits.

2.7.1.5.3 SSH Protocol Algorithms

The SSH protocol (version 2.0) is used for Remote CLI and SFTP (firmware upgrades). The approved cryptographic algorithms employed by the SSH protocol are listed in Table 10 below.

Table 10 SSH (for Remote CLI and SFTP) Cryptographic Algorithms

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

Note 1: ECDSA/ ECDH curves are restricted to NIST P-256, P-384 and P-521.

2.7.1.5.4 SNMPv3 Protocol Algorithms

The SNMPv3 protocol is used for Remote management. The approved cryptographic algorithms employed by the SNMPv3 protocol are listed in Table 11 below.

Table 11 SNMPv3 (for remote management) Cryptographic Algorithms

Algorithm Type	Algorithm
Authentication	HMAC-SHA1 HMAC-SHA256
Key Exchange	DH[1]
Symmetric Encryption	AES-128-CFB AES-256-CFB

Note 1: MODP-2048-bit Oakley Group 14 using SHA-256 for key derivation.

The Module does not implement any non-approved services when configured as per section 2.3.1 Administrator Guidance: Approved mode.

3. Cryptographic Module Interfaces

3.1 CN4000 Series Ports

3.1.1 CN4010 Ports

The CN4010 status LEDs and Emergency Erase Button are located on the module front panel.

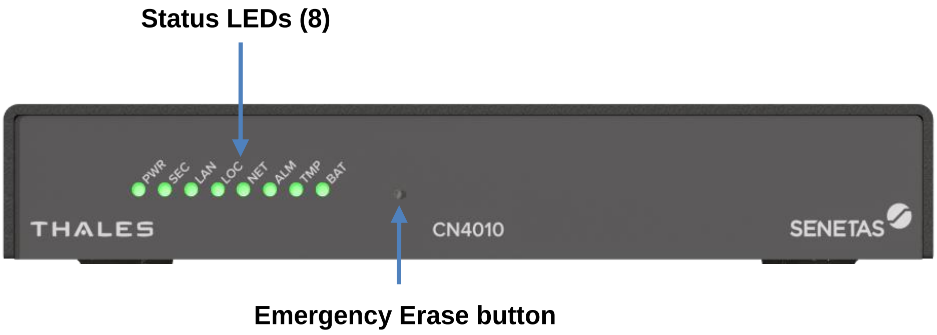


Figure 19 - Front View of the CN4010 Encryptors

The CN4010 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support electrical media in the form of RJ45 electrical physical ports. All other ports and interfaces are common to the CN4000 Series.

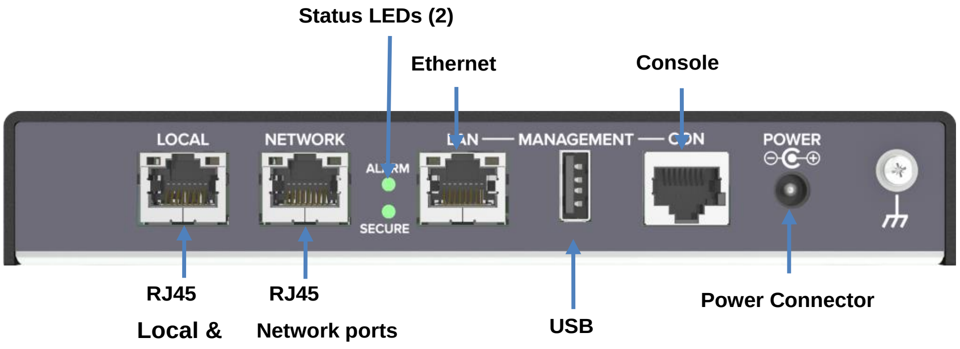


Figure 20 - Rear View of the CN4010 Encryptor

3.1.2 CN4020 Ports

The CN4020 status LEDs and Emergency Erase Button are located on the module front panel.

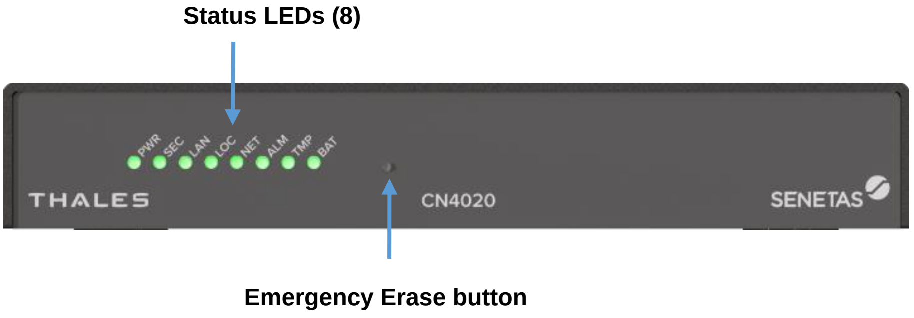


Figure 21 - Front View of the CN4020 Encryptor

The CN4020 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical media in the form of SFP optical physical ports. All other ports and interfaces are common to the CN4000 Series.

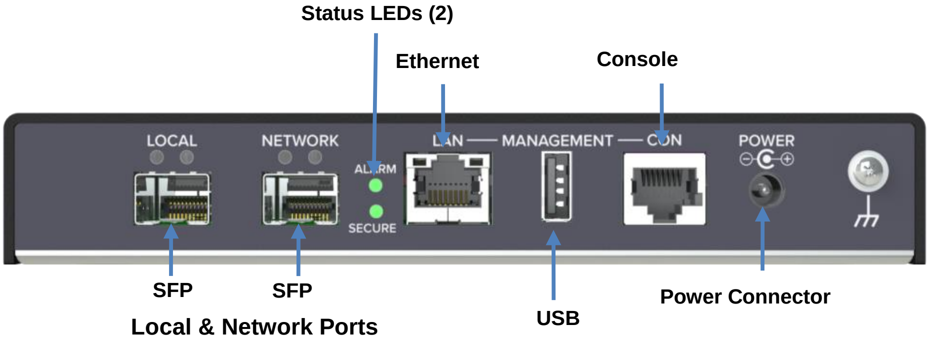


Figure 22 - Rear View of the CN4020 Encryptor

3.2 CN6000 Series Ports

3.2.1 CN6010 & CN6110 Encryptor Ports

The CN6010 & CN6110 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical or electrical media in the form of RJ45 electrical physical ports or SFP (CN6010) or SFP+ (CN6110) optical physical ports. All other ports and interfaces are common to the CN6000 Series.

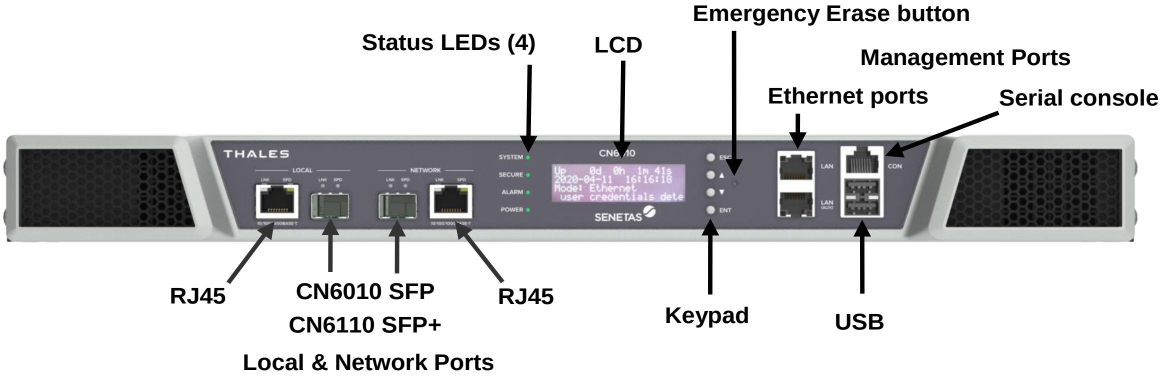


Figure 23 - Front View of the CN6010 & CN6110 Encryptor

3.2.2 CN6100 Encryptor Ports

The CN6100 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical media in the form of XFP optical physical ports. All other ports and interfaces are common to the CN6000 Series.

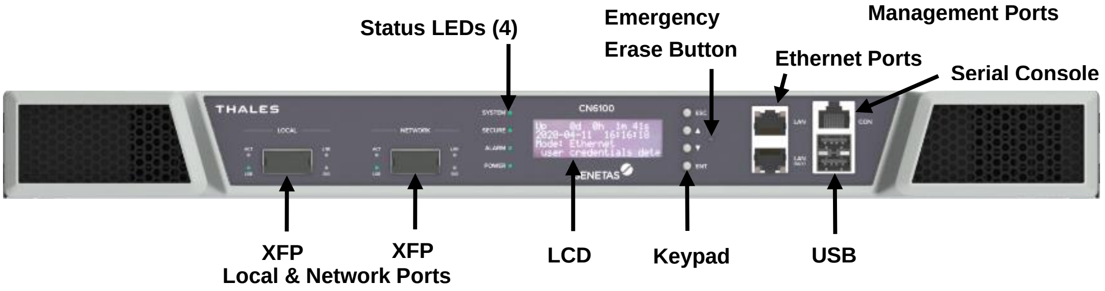


Figure 24 - Front View of the CN6100 Encryptor

3.2.3 CN6140 Encryptor Ports

The CN6140 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical media in the form of SFP+ optical physical ports. All other ports and interfaces are common to the CN6000 Series.

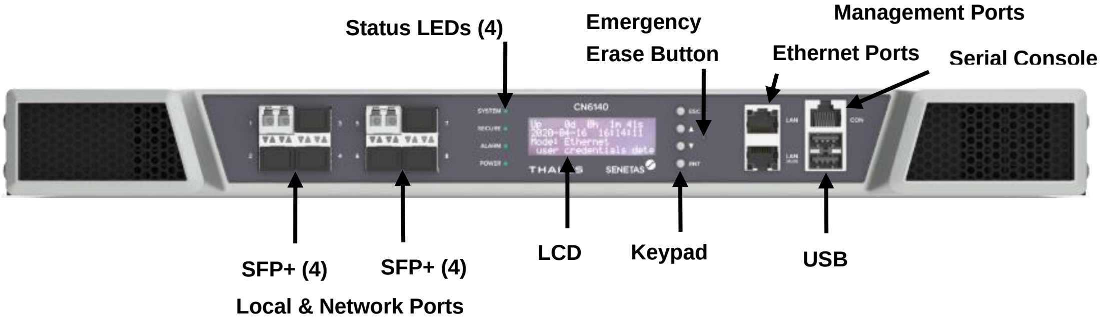


Figure 25 - Front View of the CN6140 Encryptor

3.2.4 CN6000 Series Encryptor Power Supplies and Fan Tray

The CN6000 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 26.

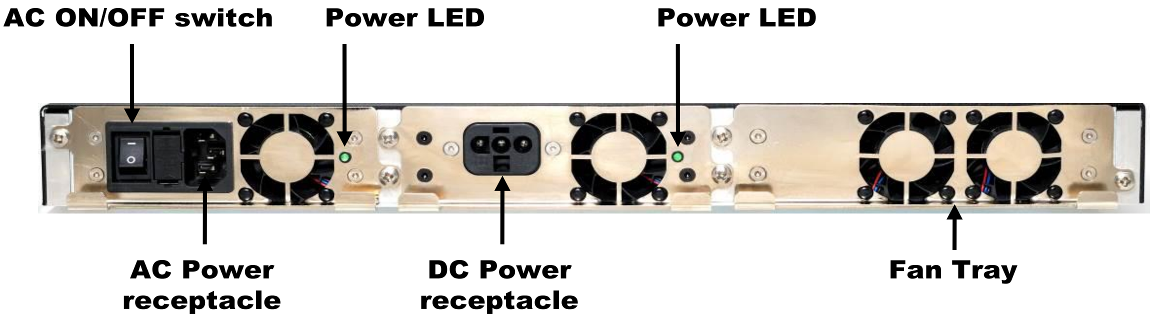


Figure 26 - Rear View: CN6000 Series Encryptor (pictured with AC & DC supplies installed)

3.3 CN9000 Series Ports

3.3.1 CN9100 Encryptor Ports

The CN9100 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical media in the form of CFP4 optical physical ports. All other ports and interfaces are common to the CN9000 Series.

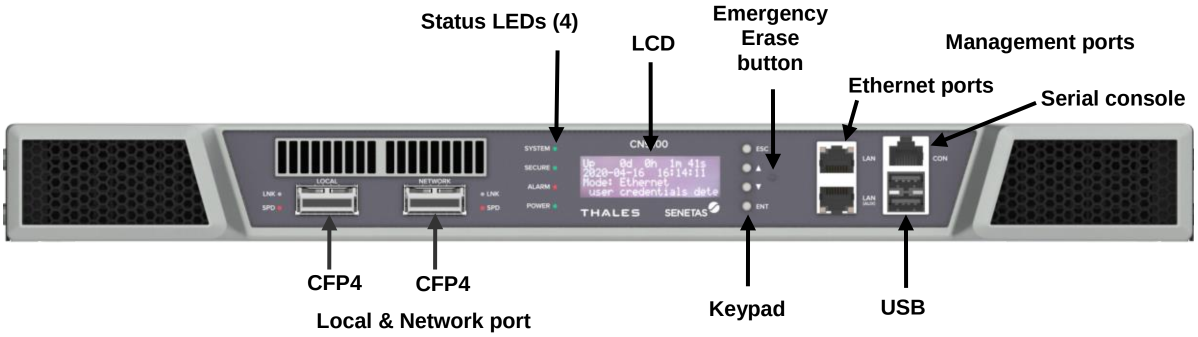


Figure 27 - Front View of the CN9100 Encryptor

3.3.2 CN9120 Encryptor Ports

The CN9120 Encryptor's Local and Network data ports, which provide connectivity between the secure and insecure network respectively, support optical media in the form of QSFP28 optical physical ports. All other ports and interfaces are common to the CN9000 Series.

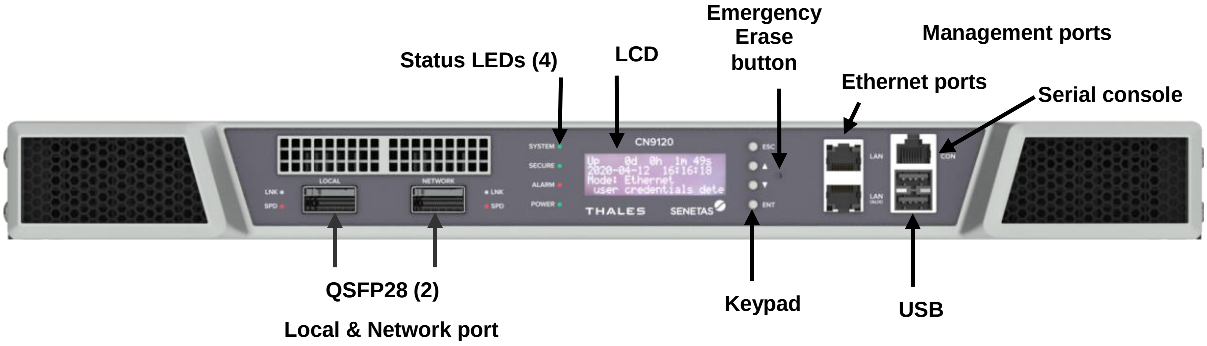


Figure 28 - Front View of the CN9120 Encryptor

3.3.3 CN9000 Series Encryptor Power Supplies and Fan Tray

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 29**.**

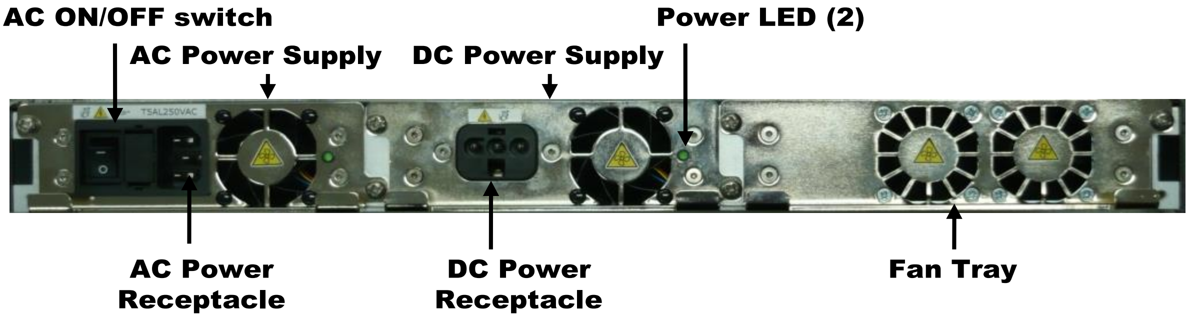


Figure 29 - Rear View: CN9000 Series Encryptor

3.4 CN Series Interfaces

Table 12 defines the CN Series interfaces and the mapping of the physical ports to the logical interfaces.

Table 12 Ports and Interfaces

Physical Port	Logical Interface[1]	Location		Data that passes over the interface
		CN4000 Series	**CN6000/ CN9000 Series**	
RJ45 Management Ethernet	Control input Status output	Rear	Front	SNMPv3 Remote CLI (SSH) Upgrade image transfer via FTP/FTPS (TLS)/SFTP (SSH) RESTful I/F (TLS) KMS (TLS)
RJ-45 RS-232 Console	Control input Status output	Rear	Front	CLI
USB	Control input	Rear	Front	Upgrade image transfer
Keypad	Control input	NA	Front	Navigation of LCD menu system and limited configuration input (Set IP address, Activation via CM7, USB upgrades)
LCD	Status output	NA	Front	Displays configuration information in response to commands entered via the keypad. Also displays system information such as boot sequence and active alarm messages
Power LED	Status output	Front	Front	Indicate powered state
System LED	Status output	NA	Front	Indicate the system operational state
Secure LED	Status output	Front/Rear	Front	Indicate the system secure state
LAN LED	Status output	Front	Front	Indicate management LAN link status and activity
Local LED	Status output	Front	Front	Indicate Local Port link status and activity
Network LED	Status output	Front	Front	Indicate Network link status and activity
Alarm LED	Status output	Front/Rear	Front	Indicate system alarm state
Temperature LED	Status output	Front	LCD	Indicate temperature warning alarm
Battery LED	Status output	Front	LCD	Indicate internal battery state
Network Port • CN4010 RJ45 • CN4020 SFP • CN6010 RJ45/SFP • CN6100 XFP • CN6110 RJ45/SFP+ • CN6140 4xSFP+ • CN9100 CFP4 • CN9120 QSFP28	Data input/output Control input Status output	Rear	Front	The Network Port connects to the public network; access is protected by X.509 certificates. Sends and receives ciphertext user data, via the public network, to and from a peer cryptographic module When in-band management is configured the Network Port may also receive control input and transmit status output
Local Port • CN4010 RJ45 • CN4020 SFP • CN6010 RJ45/SFP • CN6100 XFP • CN6110 RJ45/SFP+ • CN6140 4xSFP+ • CN9100 CFP4 • CN9120 QSFP28	Data input/output	Rear	Front	The Local Port connects to the private network; access is protected by X.509 certificates. Sends and receives plaintext user data to and from the local network
Emergency Erase button	Control input	Front	Front	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
Power connectors	Power interface	Rear	Rear	Provides power to the module, AC or DC for CN6000 and CN9000 Series and DC (via an “AC to DC” plug pack) for the CN4000 Series

Note 1: The Control Output interface was intentionally omitted from this table as the module does not implement it.

4. Roles, Services and Authentication

The cryptographic module supports four administrative privilege levels: Administrator, Supervisor, Upgrader and Operator. The Administrator role is highest (least restricted) privilege level and is authorized to access all module services. FIPS140-3 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, Supervisor or Upgrader whilst Users assume the role of an Operator.

4.1 Supported Roles

The supported roles and services are summarized in Table 13.

Table 13 Roles, Service Commands, Input and Output

Role	Service	Input	Output
Administrator (Crypto Officer)	Set Real Time Clock	Time and Date	New time and date
	Activation	New administrator credentials	Status
	Generate X.509v3 Certificate Signing Request	Certificate parameters	CSR
	Load X.509v3 Certificate	Signed certificate	Updated certificate table
	Create User Account	User details and passwords	Updated user table
	Modify User Account	User details and passwords	Updated user record
	Delete User Account	User record index	Updated user table
	View User Account	User record index	User record
	Set Global Mode (Bypass)	Global mode setting –b (Bypass)	Global Mode status
	View Global Mode	Command	Global Mode status
	Show Version	Command	Versioning info
	Clear Audit Trail	Command	Command status
	View Audit Trail	Command	Audit log
	Clear Event Log	Command	Command status
	View Event Log	Command	Event log
	Change FIPS mode status	FIPS mode setting (on/off)	Command status
	View FIPS mode status	Command	FIPS mode status
	Run Self-test (Reboot Command)	Command	Self-test status
	Install Firmware Upgrade	Signed firmware upgrade image	Updated firmware version
	Establish FTPS (TLS) Session	Session parameters	Connection success/failure
	Establish SFTP (SSH) Session	Session parameters	Connection success/failure
	Re/Start Secure Connection	Command	Connection success/failure
	Erase Module – Zeroize (Console Command)	Command	Status
	Establish a Remote Management (SNMP) Session	Session parameters	Connection success/failure
	Establish a Remote CLI (SSH) Session	Session parameters	Connection success/failure
	Establish RESTful HTTPS (TLS) Session	Session parameters	Connection success/failure
	KeyVault Sign (X.509v3 Certificate Signing Request)	CSR for signing	Signed certificate
	KeyVault Encrypt	32 Byte plaintext data block	Encrypted block
	KeyVault Decrypt	32 Byte encrypted data block	Decrypted block
	KeyVault DRBG Access	Command	32 byte output from DRBG
	KeyVault Backup	Command	PKCS12 backup file
	KeyVault Restore	Command	PKCS12 backup file
	Enable KeySecure	Command	Command status
	Generate TIM KDK	Command	TIM KDK
Supervisor (Crypto Officer)	Set Real Time Clock	Time and Date	New time and date
	View User Account	User record index	User record
	Set Global Mode (Bypass)	Global mode setting –b (Bypass)	Global Mode status
	View Global Mode	Command	Global Mode status
	Show Version	Command	Versioning info
	View Audit Trail	Command	Audit log
	View Event Log	Command	Event log
	View FIPS mode status	Command	FIPS mode status
	Run Self-test (Reboot Command)	Command	Self-test status
	Re/Start Secure Connection	Command	Connection success/failure
	Establish a Remote Management (SNMP) Session	Session parameters	Connection success/failure
	Establish a Remote CLI (SSH) Session	Session parameters	Connection success/failure
	Establish RESTful HTTPS (TLS) Session	Session parameters	Connection success/failure
Upgrader (Crypto Officer)	View User Account	User record index	User record
	View Global Mode	Command	Global Mode status
	Show Version	Command	Versioning info
	View Audit Trail	Command	Audit log
	View Event Log	Command	Event log
	View FIPS mode status	Command	FIPS mode status
	Install Firmware Upgrade	Signed firmware upgrade image	Updated firmware version
	Establish FTPS (TLS) Session	Session parameters	Connection success/failure
	Establish SFTP (SSH) Session	Session parameters	Connection success/failure
	Establish a Remote Management (SNMP) Session	Session parameters	Connection success/failure
	Establish a Remote CLI (SSH) Session	Session parameters	Connection success/failure
	Establish RESTful HTTPS (TLS) Session	Session parameters	Connection success/failure

Operator (User)	View User Account	User record index	User record
	View Global Mode	Command	Global Mode status
	Show Version	Command	Versioning info
	View Audit Trail	Command	Audit log
	View Event Log	Command	Event log
	View FIPS mode status	Command	FIPS mode status
	Establish a Remote Management (SNMP) Session	Session parameters	Connection success/failure
	Establish a Remote CLI (SSH) Session	Session parameters	Connection success/failure
	Establish RESTful HTTPS (TLS) Session	Session parameters	Connection success/failure

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 command or by performing the Erase key press sequence defined in the user guides [26]. 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 Section 3 for location on each of the models.**

4.2 Bypass Configuration

The module implements a bypass capability initiated by an authenticated user with sufficient privileges. Prior to application, the integrity of the current configuration is confirmed. After this the change is enacted by updating the static configuration and then enforcing the policy in the hardware data path controller.

Bypass configuration is evident through policy configuration.

4.3 Identification and Authentication

The module employs Identity-Based Authentication. Four operator privilege levels have been defined for use, Administrator, Supervisor, Upgrader and Operator with access rights as indicated in Table 14. 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, Upgraders and Operators) 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.

4.4 Roles and Authentication

The strength of the authentication mechanisms is detailed in Table 14

Table 14 Roles and Authentication

Role	Authentication Method	Authentication Strength
Administrator (Crypto Officer) **Supervisor (Crypto Officer)** **Upgrader (Crypto Officer)** **Operator (User)**	Identity-based	Crypto Officers and Users accessing the module CLI, via the Local Console, must authenticate using a password that is at least 8 characters and at most 29 characters in length. The characters used in the password must be from the ASCII character set of alphanumeric and special (printable) characters. This yields a minimum of 94^8 possible combinations making the possibility of correctly guessing a password 1/94^8 which is far less than 1/ 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 3/94^8 which is less than 1/100,000. Note: The module also suppresses feedback of authentication data, being entered into the Local Console, by returning * characters. Crypto Officers and Users 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.

4.5 Roles and Services

CN 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 SSPs associated with the services. The modes of access are also identified per the explanation.

Legend for access rights column in Table 15:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

N/A - Not Applicable.

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

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

4.5.1 Approved Services

The CN Series Encryptors support the approved services listed in Table 15.

Table 15 Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys or SSPs	Indicator
Set Real Time Clock		None	None	Administrator Supervisor	N/A	N/A
Activation		RSA SHA256 CKG AES-256	RSA Public Key	Administrator	G, R, E	activation status audit log
			RSA Private Key		G, E	
			Authentication Password		W	
			SMK		E	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys or SSPs	Indicator
Generate X.509v3 Certificate Signing Request		RSA ECDSA AES-256 CKG	X.509v3 Certificate, RSA Public Key, ECDSA Public Key	Administrator	G, R	command status event log
			RSA Private Key, ECDSA Private Key		G	
			SMK		E	
Load X.509v3 Certificate		RSA ECDSA	X.509v3 Certificate, RSA or ECDSA Public Key[6]	Administrator	W	certificate status audit log
Create User Account		AES-256 SHA256	Authentication Password	Administrator	W	command status audit log
			SMK		E	
Modify User Account		AES-256 SHA256	Authentication Password	Administrator	W	command status audit log
			SMK		E	
Delete User Account		None	Authentication Password	Administrator	Z	command status audit log
View User Account		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Set Global Mode (Bypass)		SHA256	None	Administrator Supervisor	N/A	command status audit log
View Global Mode		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Show Version		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Show Status		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Clear Audit Trail		None	None	Administrator	N/A	N/A
View Audit Trail		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Clear Event Log		None	None	Administrator	N/A	N/A
View Event Log		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Change FIPS mode status		None	All	Administrator	Z	command status audit log
View FIPS mode status		None	None	Administrator Supervisor Upgrader Operator	N/A	N/A
Run Self-test (Reboot Command)		None	None	Administrator Supervisor	N/A	N/A
Install Firmware Upgrade[9]		RSA SHA256	Firmware Upgrade RSA Public Key	Administrator Upgrader	E	command status audit log
		Triple-DES[10] AES-256	SMK, Authentication Passwords, Private Keys			
Establish FTPS (TLS) Session		CKG TLS v1.2 KDF (CVL) RFC5246 TLS v1.2 KDF (CVL) RFC7627 Ref. Table 8	X.509v3 Certificate, TLS Public Key	Administrator Upgrader	R, E	command status event log
			TLS Private Key		E	
			TLS Key Exchange Public Keys		G, R, E	
			TLS Key Exchange Private Keys		G, E	
			TLS Premaster Secret, TLS Master Secret[8]		G, E	
			TLS Privacy Keys[3], TLS Integrity Keys		G, E	
			SMK		E	
Establish SFTP (SSH) Session		CKG	SSH Public Key	Administrator Upgrader	E, R	command status event log
			SSH Private Key		E	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys or SSPs	Indicator
		SSH KDF (CVL) Ref. Table 10	SSH Key Exchange Public Keys		G, R, E	
			SSH Key Exchange Private Keys		G, E	
			SSH' Shared Secret[8]		G, E	
			SSH Privacy Keys[3], SSH Integrity Keys		G, E	
			SMK		E	
Re/Start Secure Connection		CKG Ref. Table 7	X.509v3 Certificate, ECDSA Public Key, RSA Public Key	Administrator Supervisor	R, W, E	command status event log
			ECDSA Private Key RSA Private Key		E	
			SME ECDH Public Key		G, R, E	
			SME ECDH Private Key		G, E	
			SME ECDH Shared Secret[8]		G, E	
			SME KDKs[1,4]. GDKs[5]		G, R, W, E	
			KEKs[1], GEKs[1], SME HMAC key		G, E	
			TIM KDK		E	
			DEKs[1]		G, R, W, E	
			SMK		E	
Erase Module – Zeroize (Console Command)			All	Administrator	Z	command status event log
Establish a Remote Management (SNMP) Session		CKG SNMP KDF (CVL) Ref. Table 11	SNMPv3 Diffie Hellman Public Keys[8]	Administrator Supervisor Upgrader Operator	G, R, E	Login status
			SNMPv3 Diffie Hellman Private Keys		G, E	
			SNMPv3 Privacy Key[2]		G, E	
Establish a Remote CLI (SSH) Session	Connect to the CLI via SSH	CKG SSH KDF (CVL) Ref. Table 10	SSH Public Key	Administrator Supervisor Upgrader Operator	E	Login status
			SSH Key Exchange Public Keys		G, R, E	
			SSH Key Exchange Private Keys		G, E	
			SSH Shared Secret		G, E	
			SSH Privacy Keys[3], SSH Integrity Keys		G, E	
Establish RESTful HTTPS (TLS) Session		CKG TLS v1.2 KDF (CVL) RFC5246 TLS v1.2 KDF (CVL) RFC7627 Ref. Table 8	X.509v3 Certificate, TLS Public Key	Administrator Supervisor Upgrader Operator	R, E	HTTPS Connection status
			TLS Private Key		E	
			TLS Key Exchange Public Keys		G, R, E	
			TLS Key Exchange Private Keys		G, E	
			TLS Premaster Secret, TLS Master Secret[8]		G, E	
			TLS Privacy Keys[3], TLS Integrity Keys		G, E	
			SMK		E	
KeyVault Sign (X.509v3 Certificate Signing Request)	Sign an X.509v3 CSR	RSA ECDSA	RSA or ECDSA Private Key SMK	Administrator	E	operation output audit log
KeyVault Encrypt	Encrypt a base64url encoded 32 byte block of plaintext.	RSA	RSA Public Key	Administrator	E	operation output

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys or SSPs	Indicator
KeyVault Decrypt	Decrypt a base64url encoded 32 byte block of ciphertext	RSA	RSA Private Key, SMK	Administrator	E	operation output
KeyVault DRBG Access	Output a 32 byte block of random data from the DRBG	DRBG	DRBG Entropy Input and Nonce, DRBG Seed, DRBG V and C	Administrator	E	operation output
KeyVault Backup	Create PKCS12 backup of public and private keys	AES256-CBC HMAC-SHA256	RSA Private/ Public Key ECDSA Private/ Public Key	Administrator	R	operation output audit log
			Password		E	
KeyVault Restore	Restore PKCS12 backup of public and private keys	AES256-CBC HMAC-SHA256	RSA Private/ Public Key ECDSA Private/ Public Key	Administrator	W	operation output audit log
			Password		E	
Enable KeySecure	Enable KeySecure connector (Ref. Section 9.3.5)	CKG TLS v1.2 KDF (CVL) RFC5246 TLS v1.2 KDF (CVL) RFC7627 Ref. Table 8	X.509v3 Certificate, TLS Public Key	Administrator	R, E	operation output audit log
			TLS Private Key		E	
			TLS Key Exchange Public Keys		G, R, E	
			TLS Key Exchange Private Keys		G, E	
			TLS Premaster Secret, TLS Master Secret		G, E	
			TLS Privacy Keys[3], TLS Integrity Keys		G, E	
			SMK_Local		G, E	
			SMK_Mask		W, E	
			SMK_CSP		G, E	
Generate TIM KDK		DRBG	TIM Key Derivation Key (KDK)	Administrator	G, R	operation output audit log
			DRBG Entropy Input and Nonce, DRBG Seed, DRBG V and C		E	

Note 1: Starting/Restarting a secure connection causes new SME KDK, GDKs, 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 SSH Privacy Keys are established using ECDH. If the firmware upgrade image is being transferred via FTPS then TLS Privacy Keys are established using ECDH. When a remote CLI session is established SSH Privacy Keys are established using ECDH.

Note 4: SME KDKs are established using Approved RSA-OAEP-256 key transport as per SP 800-56Brev2 Section 9.

Note 5: GDKs are established using ECDH key agreement.

Note 6: The Load X.509 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 7: All key material is sourced from the SP 800-90Arev1 DRBG and in accordance with FIPS 140-3 IG D.L, the entropy input string, seed and state variables V and C are considered CSPs.

Note 8: The firmware upgrade image’s signature is checked prior to installation.

Note 9: Triple-DES is only used to decrypt CSPs when upgrading from legacy versions of software. The CSPs are subsequently re-encrypted using AES-256 CFB. Triple-DES is no longer used by the module for encryption operations.

5. Software/Firmware Security

5.1 Software/Firmware Integrity Test

A 32-byte SHA-256 hash is used for each firmware component to verify the integrity of all components within the cryptographic module when the module is powered up, during the periodic test and on demand.

The original hash calculation is performed, for each module within the system, at firmware build time. The hash values are then maintained within the system. During the self-tests, the hash calculation is performed again for each module and compared with the stored values that were generated at build time. Any discrepancy will cause the self-test to fail and the module will transition to the Secure Halt state. Refer to Section 10 for further information.

5.1.1 On Demand Software/Firmware Integrity Test

The user can execute the Software/Firmware integrity test on demand by issuing the reboot command.

6. Operational Environment

Not Applicable. The operational environment of the module does not provide access to a general-purpose operating system (OS). The module employs a limited operational environment. Only signed and authenticated firmware upgrade images that pass the firmware load test can be installed on the module by authorised users.

7. Physical Security

7.1 Physical Security Mechanisms

CN Series Encryptors have a multiple-chip standalone embodiment and 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 production grade metal enclosure is opaque to the visible spectrum. All ventilation holes are factory fitted with steel 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 SSPs. For further details refer to Section 9.3.3.
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 30 (CN4000), Figure 31(CN6000) and Figure 32 (CN9000). 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.

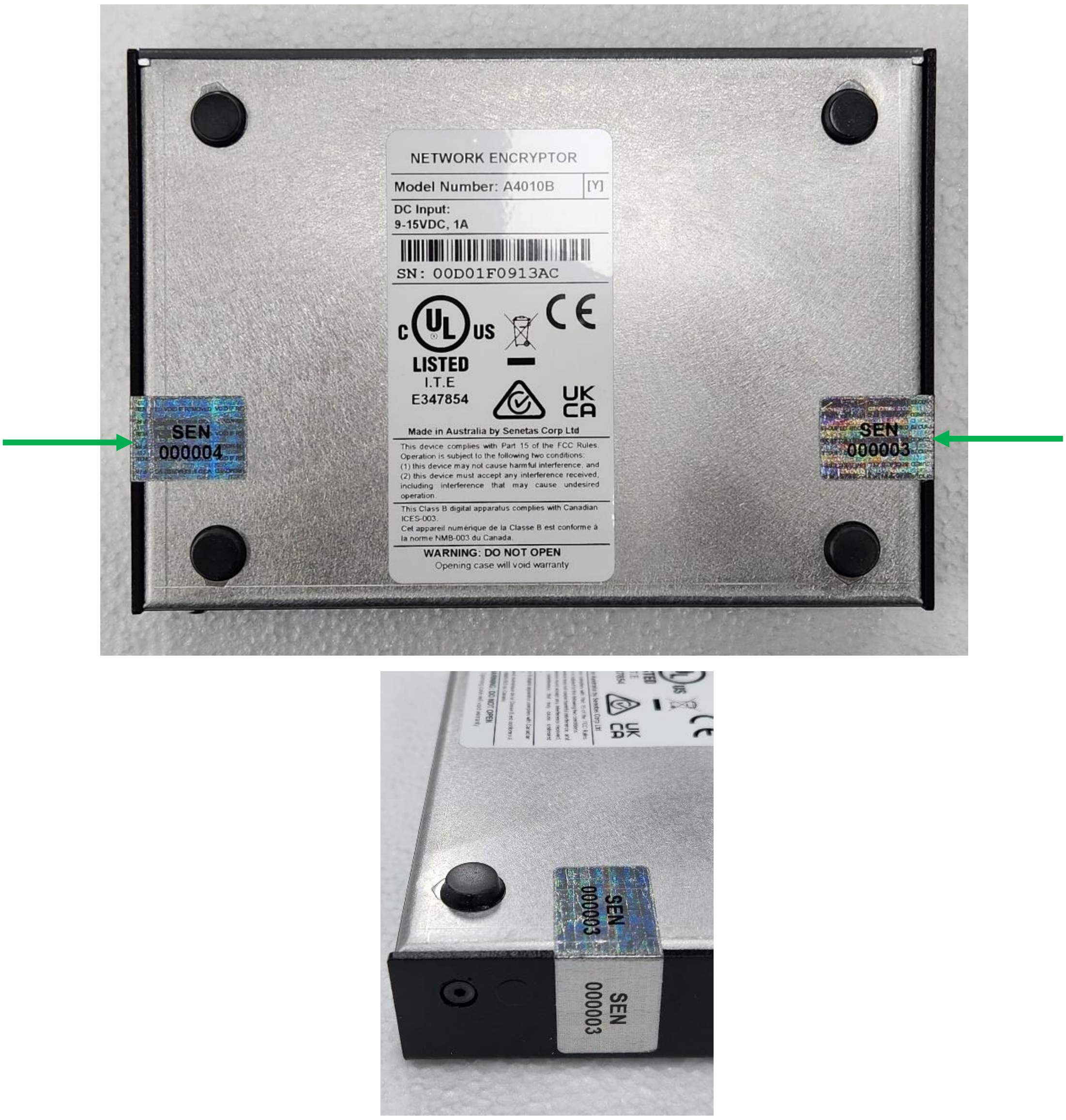


Figure 30 – CN4000 Series factory installed tamper seals

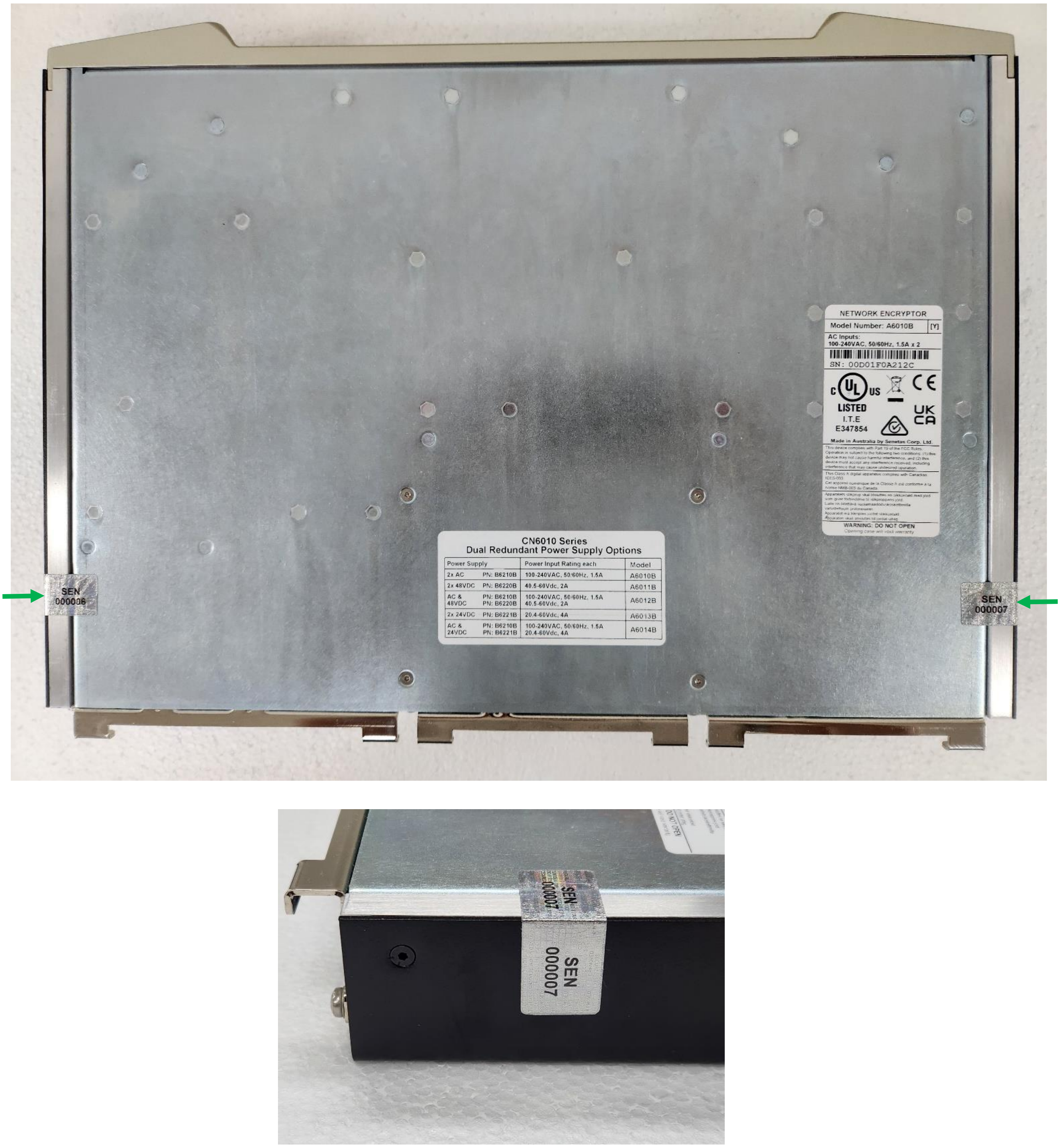


Figure 31 – CN6000 Series factory installed tamper seals

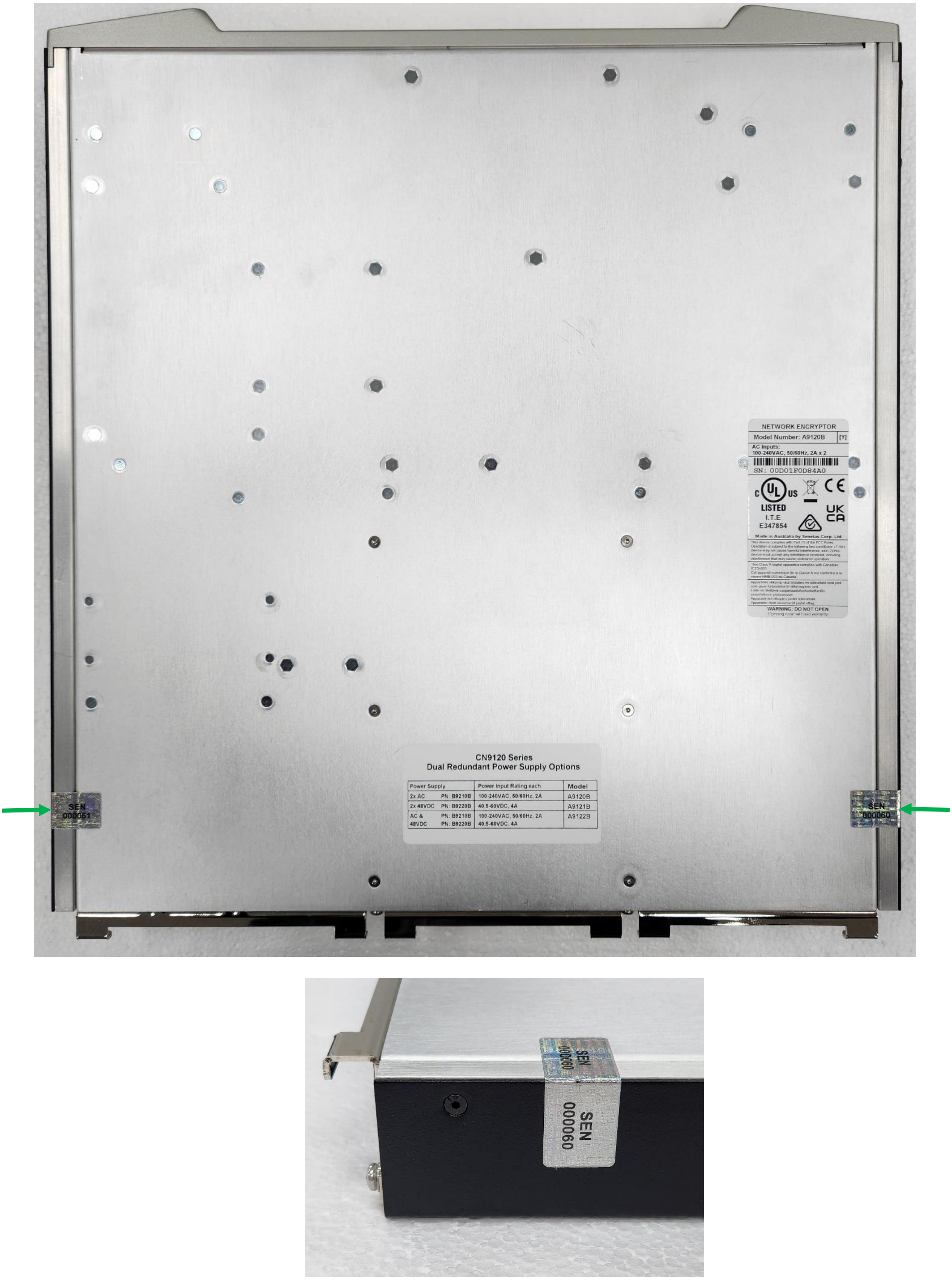

NETWORK ENCRYPTOR
Model Number: A9120B
AC Inputs: 100-240VAC, 50/60Hz, 2A x 2
SN: 00D01F0D84A0
LISTED
I.T.E
E347854
UK CA
Made in Australia by Senetas Corp. Ltd
WARNING: DO NOT OPEN
Opening cover will void warranty
CN9120 Series
Dual Redundant Power Supply Options
Power Supply
Power Input Rating each
Model
2x AC PN: B9210B 100-240VAC, 50/60Hz, 2A A9120B
2x 48VDC PN: B9220B 40.5-60VDC, 4A A9121B
AC & 48VDC PN: B9210B PN: B9220B 100-240VAC, 50/60Hz, 2A 40.5-60VDC, 4A A9122B
SEN 000061
SEN 000060
SEN 000060

Figure 32 – CN9000 Series factory installed tamper seals

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

Table 16 outlines the recommended inspection practices and/or testing of the physical security mechanisms.

Table 16 Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evidence	In accordance with the organization’s Security Policy.	Tamper indication is available to all user roles via the physical evidence of tampering against the tamper evident seals. The Crypto Officer is responsible for the physical security inspection. Inspect the enclosure and tamper evident seals for physical signs of tampering or attempted access to the cryptographic module.
Tamper Circuit	No direct inspection or test is required; triggering the circuit will block all data flow. It is recommended that the module’s alarm table is reviewed on a daily basis.	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. Tamper indication is available to all users via the alarm mechanism. 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.

7.2 Environmental Failure Protection and Testing

Environmental Failure Protection is implemented in the CN Series Encryptors for both temperature and voltage. The internal temperature and main 12VDC input voltage are constantly monitored and if the sensed values exceed the critical thresholds the encryptor will shutdown. The critical thresholds are given in Table 17 below.

Table 17 Environmental Failure Protection/Testing

CN4010	**Measurement Internal**	**EFP/EFT**	**Action (Shutdown or Zeroization)**
Low Temperature (ºC)	15	EFP	Shutdown
High Temperature (ºC)	85	EFP	Shutdown
Low Voltage (V)	9.0	EFP	Shutdown
High Voltage (V)	15.0	EFP	Shutdown
CN4020			
Low Temperature (ºC)	15	EFP	Shutdown
High Temperature (ºC)	80	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown
CN6010			
Low Temperature (ºC)	20	EFP	Shutdown
High Temperature (ºC)	85	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown

CN6100			
Low Temperature (ºC)	5	EFP	Shutdown
High Temperature (ºC)	80	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown
CN6110			
Low Temperature (ºC)	10	EFP	Shutdown
High Temperature (ºC)	80	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown
CN6140			
Low Temperature (ºC)	10	EFP	Shutdown
High Temperature (ºC)	80	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown
CN9100			
Low Temperature (ºC)	10	EFP	Shutdown
High Temperature (ºC)	85	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown
CN9120			
Low Temperature (ºC)	10	EFP	Shutdown
High Temperature (ºC)	85	EFP	Shutdown
Low Voltage (V)	10.2	EFP	Shutdown
High Voltage (V)	13.8	EFP	Shutdown

7.3 Hardness Testing Temperature Ranges

The CN Series Encryptor’s enclosures were tested across the temperature ranges detailed in **Table 18**. No perceptible deformation or change to the enclosure’s integrity occurred during testing.

Table 18 Hardness Testing Temperature Ranges

CN4000	**Hardness tested temperature measurement**
Low Temperature (ºC)	-20
High Temperature (ºC)	+80
CN6000	
Low Temperature (ºC)	-20
High Temperature (ºC)	+80
CN9000	
Low Temperature (ºC)	-20
High Temperature (ºC)	+80

8. Non-Invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation techniques referenced in SP 800-140F.

9. Sensitive Security Parameter Management

9.1 Cryptographic Keys and SSPs

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

Table 19 SSPs

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
System Master Key (SMK)[6] (CSP)	256-bit	AES-CFB AES A3451	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Persistently stored in plaintext in a tamper protected memory device	• Tamper event • Emergency erase button • Erase command	On initialization, the module generates the System Master Key (SMK). This key encrypts the module's RSA Private Key(s) and ECDSA Private Key(s) and the user passwords stored in the configuration flash memory.
Triple-DES System Master Key (CSP)	192-bit	3-key Triple-DES CFB8 Triple-DES A3451	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Stored in plaintext in a tamper protected memory device	Zeroised during upgrade process	The Triple-DES SMK is only used to decrypt CSPs when upgrading from legacy versions of firmware. The CSPs are subsequently re-encrypted using the AES SMK and the Triple-DES System Master Key is destroyed. Triple-DES is no longer used by the module for encryption operations.
SMK_Local (CSP)	256-bit	N/A	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Persistently stored in plaintext in a tamper protected memory device	• Tamper event • Emergency erase button • Erase command	When KeySecure is configured, the local System Master Key (SMK_local) is generated from the internal DRBG and stored it in tamper protected memory.
SMK_Mask (CSP)	256-bit	N/A	External	Imported from Keysecure Keyserver	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after use • Power cycle	When KeySecure is configured, the module will obtain a System Master Key mask (SMK_mask) from the external KeySecure server.
SMK_CSP (CSP)	256-bit	AES-CFB AES A3451	Internal Created by combining SMK_local and SMK_mask	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after use • Power cycle	SMK_local and SMK_mask are combined to create SMK_CSP which is used to encrypt and decrypt the module's RSA Private Key(s) and ECDSA Private Key(s) and the user passwords stored in the configuration flash memory.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
RSA Private Keys (CSP)	2048-bit	RSA SigGen RSA-OAEP-256 Key Transport RSA A3451 KTS-IFC A3451 as per IG D.G Key Transport Methods	Internal FIPS 186-4 RSA SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Persistently stored AES-256 encrypted using the System Master Key in non-volatile system memory.	- Tamper event - Emergency erase button - Erase command	Generated when the module receives a Load Certificate command from the remote management application. The RSA Private Keys are used to authenticate connections with other encryptors and to unwrap master session keys (KDK or GDK) and initial session keys (DEKs) received from far-end encryptors. KeyVault Sign: The RSA Private Keys are used to sign X.509v3 Certificate Signing Requests. KeyVault Decrypt: The RSA Private Keys are used to decrypt externally supplied session keys (KDK, GDK and initial DEKs).
RSA Public Keys (PSP)	2048-bit	RSA SigVer RSA-OAEP-256 Key Transport RSA A3451 KTS-IFC A3451 as per IG D.G Key Transport Methods	Internal FIPS 186-4 RSA SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Persistently stored plaintext in the Module Certicate(s) in non-volatile system memory.	- Tamper event - Emergency erase button - Erase command	Generated when the module receives a Load Certificate command from the remote management application. The RSA Private Keys are used to authenticate connections with other encryptors. KeyVault Encrypt: The RSA Public Key(s) are used to encrypt session keys (KDK, GDK and initial DEKs). **Note:** The module and the remote management application CM7 will only generate certificates with RSA 2048-bit key size, however It is possible to load a certificate from an external CA with RSA 4096-bit key size. The module certificate will have an RSA 2048-bit key which will be used for key wrapping the KDK, GDK and initial DEKs.
ECDSA Private Keys (CSP)	P-256 P-384 P-521	ECDSA SigGen ECDSA A3451	Internal 186-4 SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	N/A	N/A	Persistently stored AES-256 encrypted using the System Master Key in non-volatile system memory	- Tamper event - Emergency erase button - Erase command	Generated when the module receives a Load Certificate command from the remote management application. The ECDSA Private Keys are used to authenticate connections with other encryptors.
ECDSA Public Keys (PSP)	P-256 P-384 P-521	ECDSA SigVer ECDSA A3451	Internal 186-4 SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	Sent to peer encryptor during connection establishment	N/A	Stored persistently in plaintext in the Module Certificate(s) in non-volatile system memory	- Tamper event - Emergency erase button - Erase command	Generated when the module receives a Load Certificate command from the remote management application. The ECDSA Private Keys are used to authenticate connections with peer encryptors.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
SME ECDH Private Key (CSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Established during the SME key agreement process and destroyed once the process is complete. The ECDH Ephemeral Private Key is used to create the shared secret.
SME ECDH Public Key (CSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	Sent to peer encryptor during connection establishment	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Established during the SME key agreement process and destroyed once the process is complete. The ECDH Ephemeral Private Key is used to create the shared secret.
SME ECDH Shared Secret (CSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	N/A	N/A	Established during the SP 800-56Arev3 compliant ECDHE key agreement	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Generated during the SME key agreement process and destroyed after use.
X509v3 Certificates (PSP)	N/A	N/A	N/A	CSRs exported for singing by a CA Signed certificates imported	N/A	Persistently stored in plaintext, in non-volatile system memory	• Tamper event • Emergency erase button • Erase command	An X.509 certificate is associated with a session/connection in an operational environment or a service such as FTPS. Certificates used for secure connections are 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 ECDSA public key to authenticate messages sent during the ECDH key agreement process.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
Authentication Password (CSP)	8-29 ASCII characters	N/A	N/A	External Manually entered in plaintext over directly attached serial cable or via Remote CLI over SSH	N/A	AES-256-bit encrypted using the System Master Key. Stored non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	Up to 30 unique Crypto Officers (Administrators, Supervisors, Upgraders) or Users (Operators) 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.
Key Encrypting Key (KEK) (CSP)	256-bit	AES-CFB AES A3451	Internal Derived from the SME KDK using a SP 800-108rev1 compliant KDF	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	For each RSA based session (CI) and EC Multipoint sessions, the AES KEK is derived from the SME KDK using a SP 800-108rev1 compliant KDF. The KEK persists for the life of the session and is used to secure the Data Encrypting Key that may be changed periodically during the session. EC point to point connections use ECDH key agreement to generate the DEKs. In this case there is no need for KEKs.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
Data Encrypting Key (DEK) (CSP)	128-bit 256-bit	AES-CFB AES-CTR AES-GCM AES A3435 AES A3436 AES A3437 AES A3438 AES A3439 AES A3440 AES A3441 AES A3442 AES A3443 AES A3444 AES A3445 AES A3446 AES A3447 AES A3448 AES A3458 AES A3459 AES A3460 AES A3492 AES A3549	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG or Derived from a Key Derivation Key using SP 800-108rev1 compliant KDF	Approved RSA-OAEP-2048 KTS Approved AES key wrapping (KEK) authenticated with HMAC-SHA-256 Provided by an external KMIP Key Server	Approved ECDH Key Agreement	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The module generates DEKs for each data flow path in the secure connection (one for the Initiator-Responder path and another for the Responder-Initiator path). The DEKs encrypt and decrypt the user data transferred between the Encryptors. These active session keys are normally changed periodically based on the key update interval. For secure connections assigned to RSA certificates RSA-OAEP-256 KTS is used to transfer the initial DEK to a far-end module. Subsequent DEKs are transferred using AES key wrapping KEK authenticated with HMAC-SHA-256. For each ECC based connection a pair of encryptors use ECDH KAS to establish DEKs. In Transport Independent Mode each encryptor uses a single egress DEK to encrypt all secure traffic. Each encryptor maintains 2 egress DEKs one in current use and one stored for the next key update. The egress DEKs are updated every hour.
TIM KDK (CSP)	256-bit	KBKDF KBKDF A3451	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1	Distributed via CM7	N/A	AES-256-bit encrypted using the System Master Key. Stored non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	The KDK is used to derive the DEKs using a SP 800-108 compliant KDF.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
Group Establishment Key (GEK) (CSP)	256-bit	AES-CFB AES A3451	Internal Derived from the GDK using an SP 800-108rev1 compliant KDF	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The GEK is used to wrap the group SME KDKs and initial DEKs using AES-256 CFB authenticated with HMAC-SHA-256.
SME HMAC keys (CSP)	256-bit	HMAC-SHA-256 HMAC A3451	Internal Derived from the GDK using an SP 800-108rev1 compliant KDF	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The SME HMAC keys are used to protect the integrity of the AES key wrapped messages between encryptors.
SME KDK (CSP)	256-bit	KBKDF KBKDF A3451	Internal SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG	Approved RSA-OAEP-2048 KTS Approved AES key wrapping (GEK) authenticated with HMAC-SHA-256.	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	For each RSA based session (CI), the module generates a 256-bit SME KDK. The SME KDK is used to separately derive the KEK and the SME HMAC keys using an SP 800-108 compliant KDF. RSA Key transport is used to transfer this key to a far-end module. EC Multipoint connections use the GEK and AES keywrap to transport the KDK.
Group Derivation Key (GDK) (CSP)	256-bit	KBKDF KBKDF A3451	N/A		ECDH Key Agreement	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	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 GDK that is used to separately derive the GEK and the SME HMAC keys using a SP 800-108rev1 compliant KDF.
SNMPv3 Privacy Keys (CSP)	128-bit 256-bit	AES-CFB AES A3451	N/A	N/A	Allowed SNMP protocol derivation	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	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.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
SNMPv3 Diffie Hellman Private Keys (CSP)	2048-bit	DH KAS-FFC A3451	N/A	N/A	Diffie-Hellman Key Agreement	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	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.
SNMPv3 Diffie Hellman Public Keys (PSP)	2048-bit	DH KAS-FFC A3451	N/A	N/A	Diffie-Hellman Key Agreement	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	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.
DRBG Seed (CSP)	440-bit	DRBG	Internal from: ESV (P): CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120 ESV (NP): CN6100	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Used for SP 800-90rev1 Hash_DRBG the 440-bit seed (initial V or state) value internally generated from nonce along with entropy input.
DRBG Entropy Input and Nonce (CSP)		DRBG	Internal from: ESV (P): CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120 ESV (NP): CN6100	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Used for SP 800-90rev1 Hash_DRBG as input to the instantiate function.
DRBG V and C internal state parameters (CSP)		DRBG	Internal	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The V and C parameters store the internal state of the SP 800-90rev1 DRBG.
SSH Private Key (CSP)	P-256 P-384 P-521	ECDSA SigGen ECDSA A3451	Internal 186-4 SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG External	N/A	N/A	Persistently stored AES-256 encrypted using the System Master Key in non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	Used to authenticate the module with the remote client/server.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
SSH Public Key (PSP)	P-256 P-384 P-521	ECDSA SigVer ECDSA A3451	Internal 186-4 SP 800-133rev2 Key Generation using SP 800-90Arev1 DRBG External	Loaded electronically onto/out of the module via CM7 or the CLI	N/A	Stored persistently in non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	Used to authenticate the module with the remote client/server.
SSH Key Exchange Private Keys (CSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The key is created for each SSH session to enable agreement of the SSH shared secret between the module and the remote client/server.
SSH Key Exchange Public Keys (PSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	Sent to SSH remote client/server	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The key is created for each SSH session to enable agreement of the SSH shared secret between the module and the remote client/server.
SSH Shared Secret (CSP)	P-256 P-384 P-521	SSH KDF CVL A3451	N/A	N/A	Established during the SP 800-56Arev3 compliant ECDHE key agreement	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Used to derive the SSH Privacy and Integrity Keys.
SSH Privacy Keys (CSP)	128-bit 256-bit	AES-CTR AES A3451	Derived from the SSH Shared Secret	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Generated during the SSH I key agreement process and used for encryption of the data transmitted across the secure SSH connection.
SSH Integrity Keys (CSP)	256-bit 512-bit	HMAC-SHA-256 HMAC-SHA-512 HMAC A3451	Derived from the SSH Shared Secret	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The SSH Integrity keys are used to protect the integrity of the data transmitted across the secure SSH connection.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
TLS Private Key (CSP)	P-256 P-384 P-521	RSA SigGen RSA A3451 ECDSA SigGen ECDSA A3451	External	Loaded electronically onto the module via CM7 or the CLI	N/A	Persistently stored AES-256 encrypted using the System Master Key in non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	Used to authenticate the module with the remote server.
TLS Public Key (PSP)	P-256 P-384 P-521	RSA SigVer RSA A3451 ECDSA SigVer ECDSA A3451	External	Loaded electronically onto the module via CM7 or the CLI	N/A	Stored persistently in non-volatile system memory.	• Tamper event • Emergency erase button • Erase command	Used to authenticate the module with the remote server.
TLS Key Exchange Private Keys (CSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The key is created for each TLS session to enable agreement of the TLS shared secret between the module and the remote server.
TLS Key Exchange Public Keys (PSP)	P-256 P-384 P-521	ECDH KAS ECC A3451	Internally generated using SP 800-90Arev1 DRBG according to SP 800-133rev2 and SP 800-56Arev3	Sent to TLS server	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The key is created for each TLS session to enable agreement of the TLS shared secret between the module and the remote server.
TLS Premaster Secret (CSP)	384-bit	TLS v1.2 KDF RFC5246/RFC7627 CVL A3451	N/A	N/A	Established during the SP 800-56Arev3 compliant ECDHE key agreement	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The TLS Premaster Secret is used to generate the TLS Master Secret.
TLS Master Secret (CSP)	384-bit	TLS v1.2 KDF RFC5246/RFC7627 CVL A3451	Derived from the TLS Premaster Secret	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The TLS Master Secret is used to derive TLS Privacy and Integrity keys.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
TLS Privacy Keys (CSP)	128-bit 256-bit	AES-CBC AES-GCM AES A3451	Derived from the TLS Master Secret	N/A	N/A	Stored ephemerally in plaintext, in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	Generated during the TLS key agreement process and used for encryption of the data transmitted across the secure TLS connection.
TLS Integrity Keys (CSP)	256-bit 384-bit	HMAC-SHA-256 HMAC-SHA-384 HMAC A3451	Derived from the TLS Master Secret	N/A	N/A	Stored ephemerally in volatile system memory	• Tamper event • Emergency erase button • Zeroized after session establishment • Power cycle	The TLS Integrity keys are used to protect the integrity of the data transmitted across the secure TLS connection.
Firmware Upgrade RSA Public Key (PSP)	2048-bit	RSA SigVer RSA A3451	External	N/A	N/A	Stored in non-volatile system memory.	N/A. This public key is embedded in the firmware.	The Firmware Upgrade RSA Public Key is the public component of the 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.

Note 1: While the certificates, maintained within the module, are listed as SSPs, they contain only public information and cannot be modified once loaded.
Note 2: As per SP 800-133rev2, all random data including cryptographic Key material is sourced unmodified from the NIST SP 800-90Arev1 DRBG as required.
Note 3: Switching modes or 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 6: The System Master Key is never used for key wrapping for transporting keys.
Note 7: The module generates entropy in 256-bit blocks. Each 256-bit block contains full entropy

.

9.2 Entropy

9.2.1 Entropy CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120

The CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120 models employ a hardware based (physical) true random number generator (RNG) that has been validated for compliance with SP 800-90B. Based on noise source testing and analysis, the estimated minimum amount of entropy per output bit is 1.0 bits. The overall amount of generated entropy meets the required security strength of 256 bits based on the entropy per bit and the amount of entropy requested by the module.

Table 20 Non-Deterministic Random Number Generation Specification CN4010, CN4020, CN6010, CN6110, CN6140, CN9100 & CN9120

Entropy Sources	Minimum number of bits of entropy	Details
ESV #E51	256 bits	The module employs a hardware based random bit generator

9.2.2 Entropy CN6100

The CN6100 employs a software based (non-physical) true random number generator (RNG) that has been validated for compliance with SP 800-90B. Based on testing and analysis, the estimated minimum amount of entropy per output bit is 1.0 bits. The overall amount of generated entropy meets the required security strength of 256 bits based on the entropy per bit and the amount of entropy requested by the module.

Table 21 Non-Deterministic Random Number Generation Specification CN6100

Entropy Sources	Minimum number of bits of entropy	Details
ESV #E49	256 bits	The module employs a software based random bit generator

9.3 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 9.3.1 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. Physically tampered

The following sections describe the specific events that occur when zeroization initiated.

9.3.1 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, TIM KDK, User passwords and other CSPs (Certificates, RSA public keys) indecipherable
- Deletes all Certificate information
- Deletes RSA and ECDSA Private and Public keys, TIM KDK, module Configuration and User passwords
- Automatically REBOOTs the module destroying KEKs, DEKs, Privacy and Diffie Hellman keys residing in volatile system memory

9.3.2 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 key press Erase sequence.

Zeroization of the module Keys and CSPs is achieved using the zeroization sequence as defined in Section 9.3.1.

9.3.3 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, TIM KDK, User passwords 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 zeroized 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 2.3).

9.3.4 "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 9.3.3 Tamper initiated zeroization above.

9.3.5 KeySecure Connector integration (Split Key SMK)

The CN Series Encryptors have the ability to communicate with SafeNet's KeySecure key management system. When KeySecure is enabled and correctly configured the encryptor will still derive a local System Master Key (SMK_local) from the internal DRBG and store it in tamper protected memory. In addition, it will also obtain a System Master Key mask (SMK_mask) from the external KeySecure server. When the encryptor needs to encrypt or decrypt a CSP it will retrieve SMK_local and SMK_mask and combine them to create SMK_CSP which is used to perform the crypto operation.

This feature allows centralised management of CSPs within a network of encryptors. Deleting SMK_mask in the KeySecure server will effectively destroy the CSPs in the encryptor. The KeySecure feature is disabled by default.

Please note that throughout this Security Policy SMK can be used to refer to both the SMK and the SMK_CSP as they both perform the same function even though they have different generation methods.

9.4 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.

10. Self-tests

CN Series Encryptors perform pre-operational, conditional and periodic self-tests to verify the integrity and correct operational functioning of the encryptor.

10.1 Pre-operational Self-tests

A set of pre-operational self-tests are executed during the power up sequence. The design of the CN Series cryptographic modules ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational 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. The pre-operational self-tests are detailed in Table 22.

Failure of the Software/Firmware integrity 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. The SHA256 algorithm is tested using a known answer test prior to it being used for the Software/Firmware integrity self-test.

Upon successful completion of the pre-operational self-tests the module will allow access via the CLI and remote management tools. The LCD will display a message stating that the self-tests passed. The data-plane ports will be enabled and normal operation will commence.

10.1.1 Periodic Self-tests

A subset of the pre-operational tests run periodically. The bypass/encrypt policy test, software/firmware integrity test are scheduled to run every 24 hours. The critical function tests run continuously. The action taken upon failure of a periodic self-test is context dependant.

10.1.2 On demand Self-tests

Crypto Officers can run the pre-operational self-tests 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.

10.2 Conditional Self-tests

A set of conditional self-tests run when required. The action taken upon failure of a conditional self-test is context dependant. The conditional self-tests are described in Table 22

The conditional cryptographic algorithm known answer tests are run during the power up sequence. Failure of a cryptographic algorithm known answer 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 22 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. Indication: LEDs flashing red (all models) and alarm message on LCD (CN6000 and CN9000 Series)
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
Pre-Operational Tests	**Performed at power-up**	
Pre-Operational Software/ Firmware Integrity	A 32-byte SHA-256 hash is used to verify the integrity of all components within the cryptographic firmware when the module is powered up and on demand by issuing the reboot command. The SHA256 algorithm is tested using a KAT prior to the Software/Firmware integrity test running. Upon any file error the system will enter a Secure shutdown state and Halt ("Secure Halt")	Halt
Pre-Operational Bypass/Encrypt Policy	The Bypass/Encrypt Policy test ensures that the Bypass/Encrypt policy setting is observed by the encryption datapath and that a frame cannot be spuriously transmitted in bypass (plaintext) when it should have been encrypted (and vice versa). In the event the test fails a log message will be generated and the global policy will be set to Discard.	Error
Pre-Operational Critical Function tests		
RTC/ Tamper	Tamper memory is examined for evidence of a Tamper Condition. If the tamper event cannot be cleared, indicating a persistent tamper state, the module transitions to the Secure Halt state	Halt
Conditional Tests	**Performed, as needed, during operation**	
Conditional Cryptographic Algorithm Tests	Each cryptographic algorithm, employed by the encryptor, is tested using a "Known Answer Test" to verify the operation of the function.CN Series KATs are divided into 19 distinct modules which correspond to the common modules listed in Table 2 and firmware modules listed in Table 6. The cryptographic KATs are run during the power up sequence.	
CN Series Common Crypto Library	The following CN Series Common Crypto Library algorithms are tested: AES128 CFB encrypt, AES128 CFB decrypt, AES256 CFB encrypt, AES256 CFB decrypt, AES-CBC-128 encrypt, AES-CBC-128 decrypt, AES-CBC-256 encrypt, AES-CBC-256 decrypt AES-GCM-128 encrypt, AES-GCM-128 decrypt, AES-GCM-256 encrypt, AES-GCM-256 decrypt, Triple-DES168 decrypt, SHA-1, SHA-256, SHA-384, SHA-512, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, KDF CTR HMAC-SHA256, RSA2048 encrypt, RSA2048 decrypt, RSA4096 encrypt, RSA4096 decrypt, RSA-OAEP-SHA-256 2048 encrypt, RSA-OAEP-SHA-256 2048 decrypt, RSA2048 Sign and Verify, RSA4096 Sign and Verify, ECDSA P-256, P-384, and P-521 (Sign and Verify and KAT), ECDH P-256, P-384, and P-521 (primitive KAT), SP 800-90Arev1 DRBG KAT, Statistical, Instantiate, Reseed, Generate and Un-instantiate tests, ECDH (Cofactor) Ephemeral Unified Model SP 800-56Arev3, DH dhEphem 2048 MODP group SP 800-56Arev3, KDF-135 SNMP KAT, KDF-135 TLS KAT, KDF-135 SSH KAT	Halt
Firmware Algorithms	CN4010 1G Ethernet; AES CFB (e/d; 128, 256), CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN4010 TIM 1G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN4020 1G Ethernet; AES CFB (e/d; 128, 256), CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN4020 TIM 1G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6010 1G Ethernet; AES CFB (e/d; 128, 256), CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6010 TIM 1G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6100 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6100 TIM 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6110 1G Ethernet; AES CFB (e/d; 128, 256), CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6110 TIM 1G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6110 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6110 TIM 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6140 1G Ethernet; AES CFB (e/d; 128, 256), CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6140 TIM 1G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6140 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6140 TIM 10G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN6140 TIM 4x10G Ethernet; AES CTR (e/d; 128, 256)	Halt
	CN9100 100G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
	CN9120 100G Ethernet; AES CTR (e/d; 128, 256), GCM (e/d; 128, 256)	Halt
Entropy Related Health Tests	The entropy source is tested using adaptive proportion and repeat count tests compliant with SP 800-90B Section 4.4 during the start-up sequence and then continuously.	Reboot
Conditional Bypass Tests		
Conditional Bypass Integrity	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-byte SHA-256 hash). Conditional bypass tests are enforced by checking the integrity during each process initialisation that memory maps specific configuration data. If the	Erase

	Hash 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 hash value.	
Conditional Bypass/Encrypt Policy	The Bypass/Encrypt Policy test ensures that the Bypass/Encrypt policy setting is observed by the encryption datapath and that a frame cannot be spuriously transmitted in bypass (plaintext) when it should have been encrypted (and vice versa). This test is performed after any change to policy. In the event the test fails a log message will be generated and the global policy will be set to Discard causing all data transmission to stop.	Error
Conditional 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 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. ECDH Public and Private keys are used for SP 800-56Arev3 approved key agreement. These keys are tested at the time they are used with a pair-wise consistency test. DH Public and Private keys are used for SP 800-56Arev3 approved key agreement. These keys are tested at the time they are used with a pair-wise consistency test.	Discard Key
Conditional Software/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
Conditional Critical Function Tests	**Performed continuously**	
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 continuously for evidence of a Tamper Condition.	Reboot

11. Life-cycle Assurance

This section provides information for Crypto Officers to install, configure and operate the CN 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.

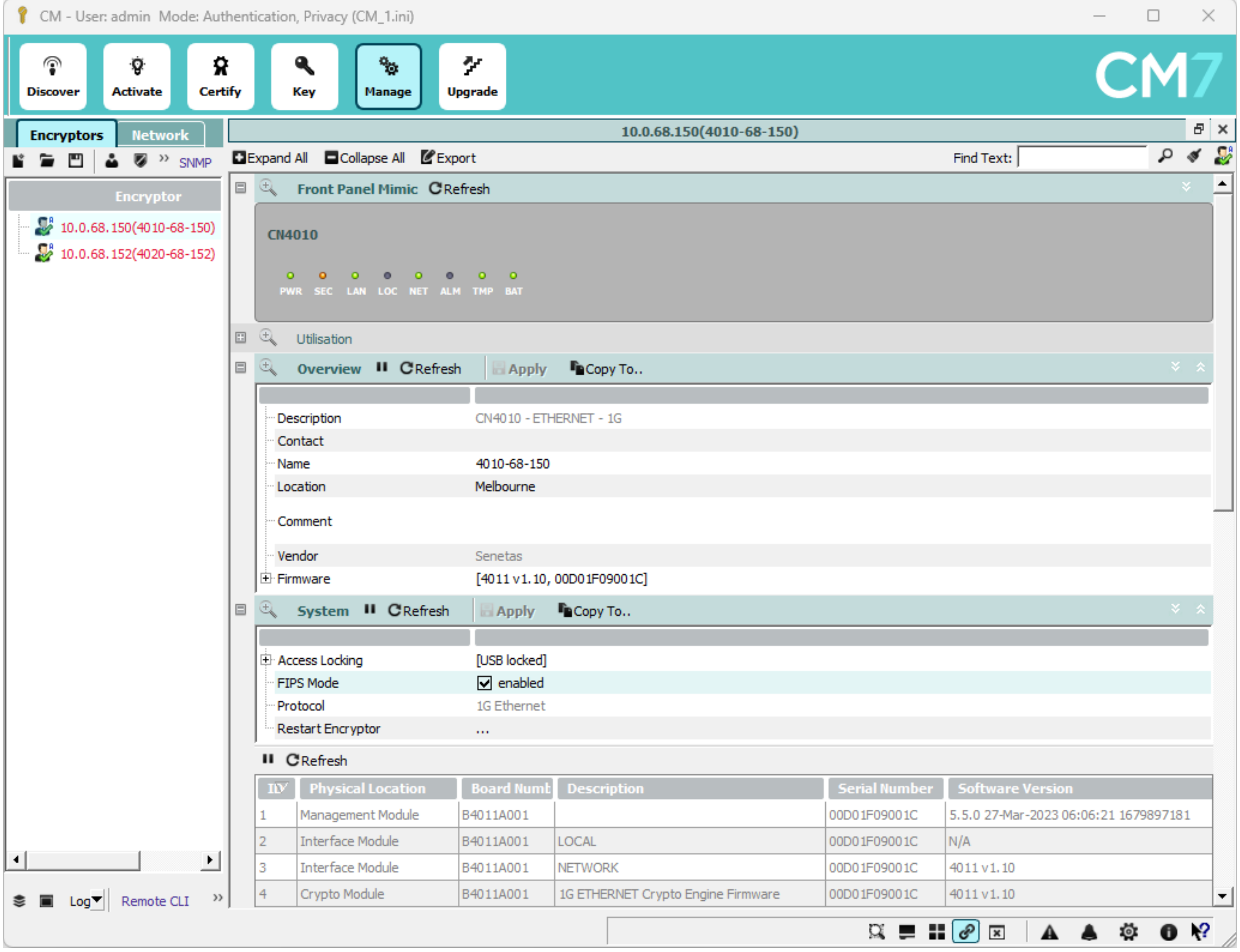
The CN Series is designed to operate in an approved mode. The operator can query the FIPS status (operating mode) of a module, and authorized operators may change the FIPS mode of operation. The FIPS status can be queried from the Local Console via the CLI or remotely via the remote management application.

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

The console command is:

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

The Senetas CM7 remote management application screen for reporting the FIPS status is found on the User Management screen, in the System pane under FIPS Mode. All of the versioning information is also displayed.



Description CN4010 - ETHERNET - 1G
Contact
Name 4010-68-150
Location Melbourne
Comment
Vendor Senetas
Firmware [4011 v1.10, 00D01F09001C]

Access Locking [USB locked]
FIPS Mode ☑ enabled
Protocol 1G Ethernet
Restart Encryptor ...

ID	Physical Location	Board Numt	Description	Serial Number	Software Version
1	Management Module	B4011A001		00D01F09001C	5.5.0 27-Mar-2023 06:06:21 1679897181
2	Interface Module	B4011A001	LOCAL	00D01F09001C	N/A
3	Interface Module	B4011A001	NETWORK	00D01F09001C	4011 v1.10
4	Crypto Module	B4011A001	1G ETHERNET Crypto Engine Firmware	00D01F09001C	4011 v1.10

Figure 33 – "FIPS mode" selection

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

11.1 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 CN 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 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.

11.2 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 CN 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.

11.3 End of Service Life

As outlined in NIST SP 800-88 Revision 1; for secure destruction of networking devices at the end of their service life:

- Zeroise the encryptor by running the CLI erase –f command or by pressing the emergency erase button which is accessible via the front panel using a paper clip.
- Shred to <2mm (.07”) squared particles or less, Disintegrate, Pulverise or Incinerate by burning the encryptor in a licensed incinerator.

12. Mitigation of Other Attacks

The CN4000 Series and CN6000 Series can be configured to mitigate against traffic analysis attacks on point-to-point connections using the TRANSEC feature.

The module does not mitigate against any other specific attacks.

12.1 TRANSEC

Traffic Analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. TRANSEC is transmission security and is used to disguise patterns in network traffic to prevent Traffic Analysis.

A TRANSEC enabled module exhibits the following encryption characteristics:

- Generates and transmits fixed size encrypted Ethernet frames at a constant frame rate from the WAN facing network port.
- Encrypts the entire Ethernet frame received on the local port so that no MAC addresses, other header information or payload data is exposed.
- The rate of the transmitted Ethernet frame is constant and independent of the received plaintext traffic rate from the local port.
- In the absence of user data from the local port the TRANSEC encryptor module fills the transmitted frames with pseudo random or encrypted data such that it cannot be distinguished from encrypted user data.
- TRANSEC encryptor modules default to decrypting traffic received on their network interface and discard all introduced traffic that is not ‘real’ user data.