Senetas Corporation Ltd, distributed by Thales SA (SafeNet)
CN Series Encryptors

FIPS 140-3 Non-Proprietary Security Policy
Document Version 1.00
16 June 2026

Table of Contents

List of Tables

List of Figures

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) 800-140Brev1 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) 800-140F 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*

Acronyms and Abbreviations

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
APT	Adaptive Proportion Test
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
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
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
RBG	Random Bit Generator
RCT	Repeat Count Test
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
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 General

1.1 Overview

This is a non-proprietary FIPS 140-3 Security Policy for the Senetas Corporation Ltd. CN Series Encryptors (running firmware version 5.5.0/5.5.1) 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.

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 CN4010, CN4020, CN6010, CN6100, CN6110, CN6140, CN9100 and CN9120 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 Encryptors” 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).

This Security Policy and the associated CMVP certificate are for firmware 5.5.0/5.5.1 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 Encryptors systems, visit https://www.senetas.com.

1.2 Security Levels

The module meets the overall Security Level 3 requirements for FIPS 140-3. The table below reflects the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

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
	Overall Level	3

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

CN Series Encryptors operate in point-to-point and point-to-multipoint network topologies 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.

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'.

The 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 with 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 11.2 Administrator Guidance 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.

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

Figure 1 illustrates the conceptual data flow through the encryptor.

1. A data packet arrives at the encryptor's interface ports. When operating in Line mode data packets are processed according to a single CI policy, otherwise,
2. The encryptor looks up the appropriate packet header field, e.g. 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.

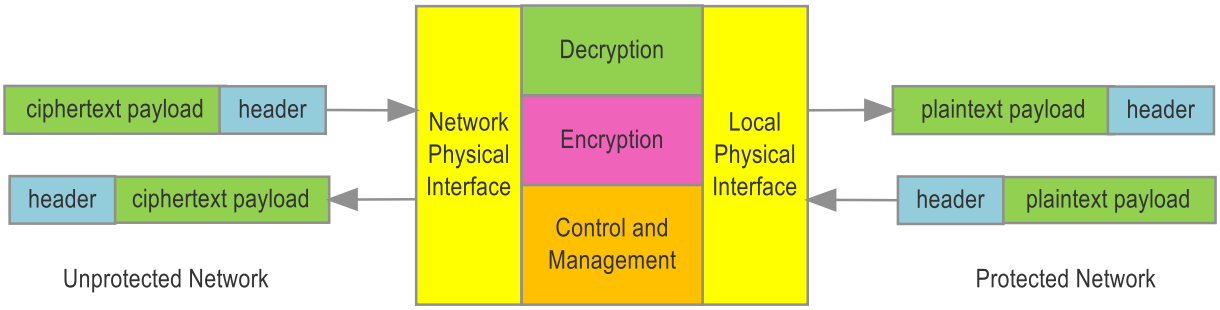

Figure 1 – Data Flow through the Encryptor

Encryptor deployment

Figure 2 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, a separate pair of encryptors needs to be deployed for each physical connection (link).

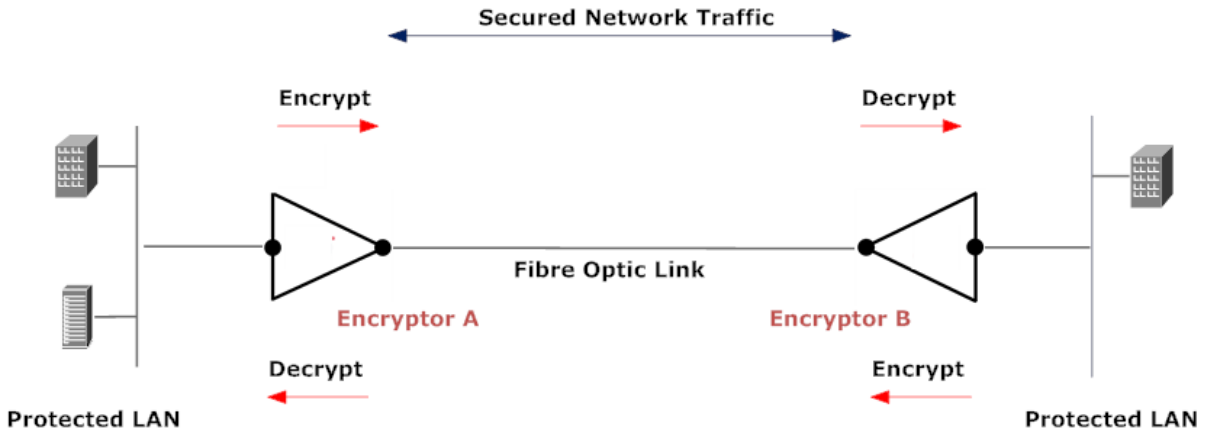

Figure 2 – Link (point-to-point) Configuration

Figure 3 illustrates a meshed network configuration. Each module is able to maintain simultaneous secured connections with many far end encryptors.

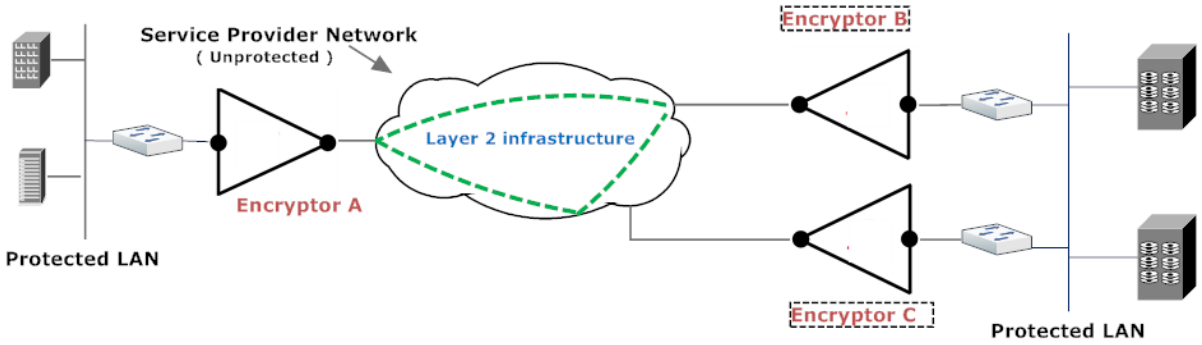

Figure 3 – Meshed (multipoint) Configuration

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 Management 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.

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

Ethernet implementation

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 4 below.

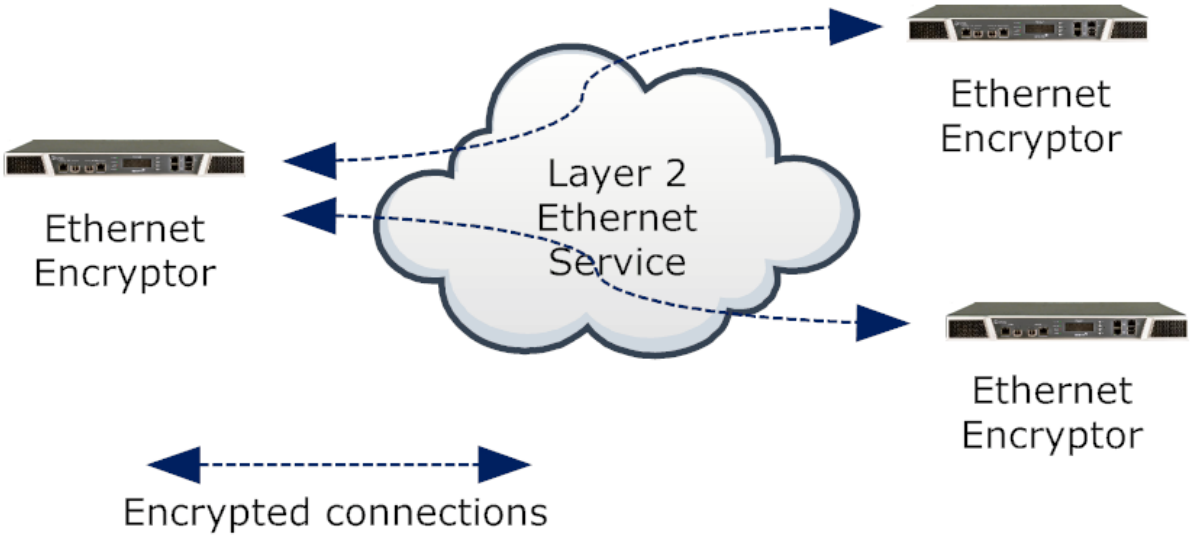

Figure 4 – Layer 2 Ethernet connections

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.

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.

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.

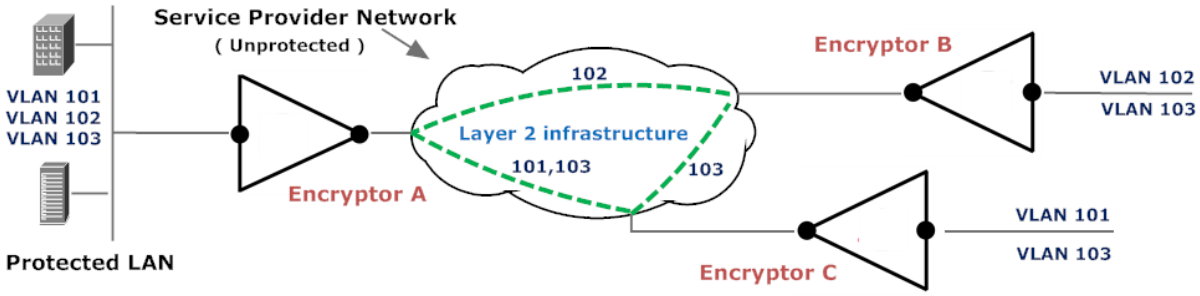

Figure 5 – Multipoint VLAN connections

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.

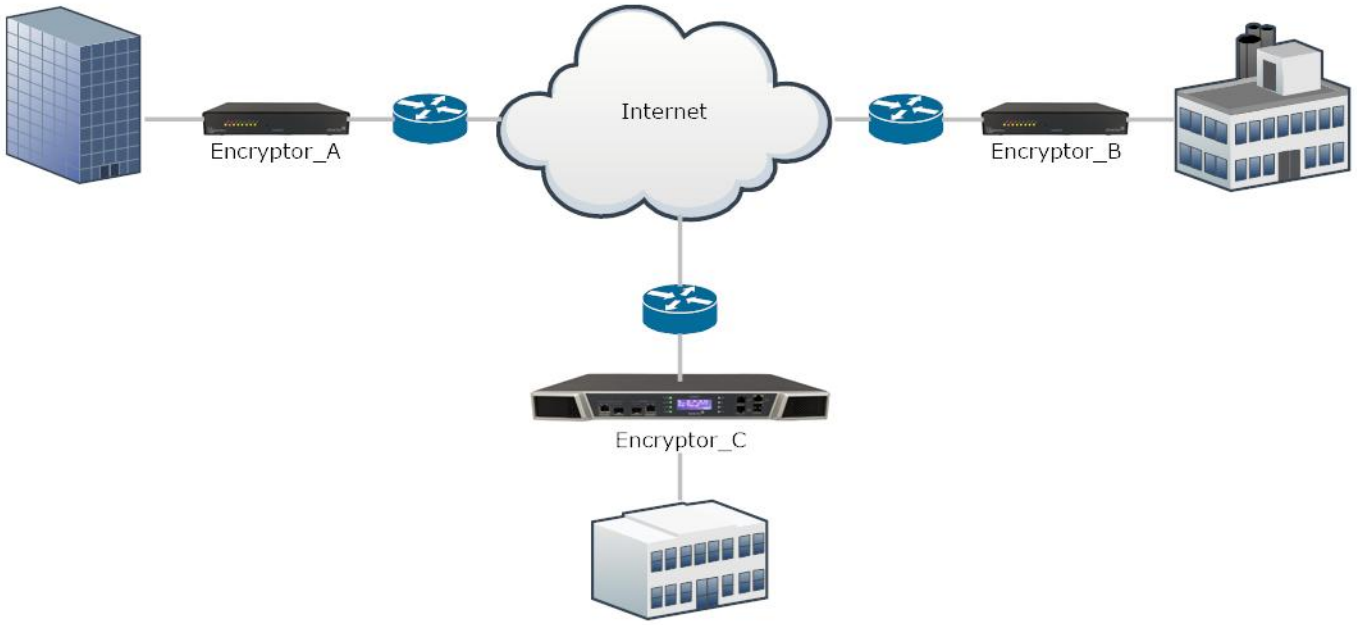

Figure 6 – Transport Independent Mode connections

Hybrid Session Establishment

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

Quantum Resistant Algorithms (QRA)

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

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.

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.

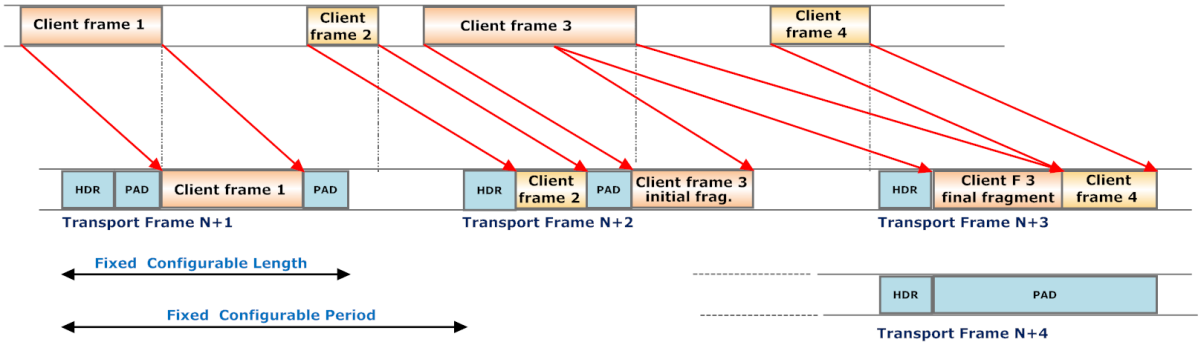

Figure 7 – TRANSEC constant rate transport frame assembly

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The 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 8 below.

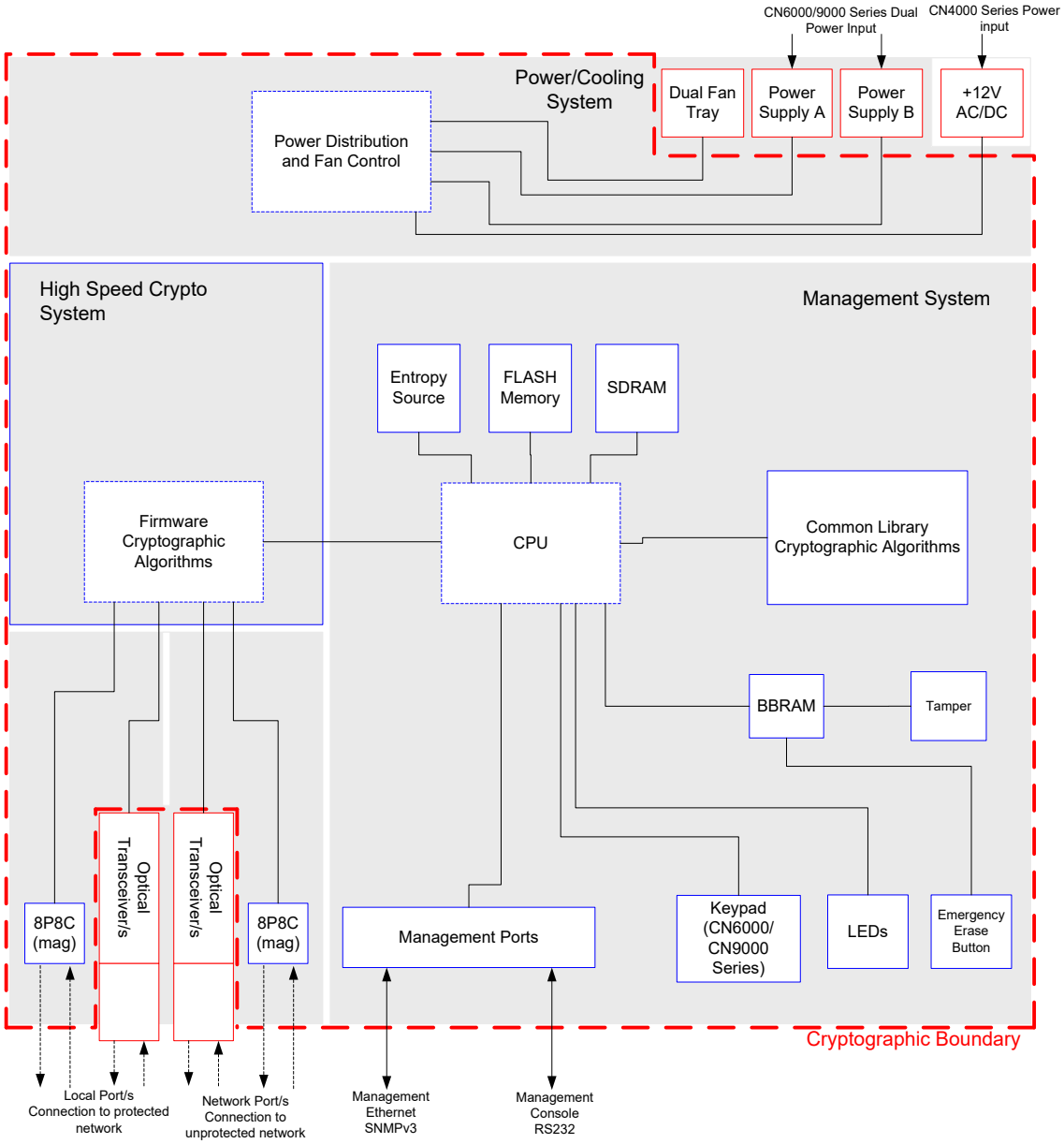

Figure 8 – Cryptographic Boundary Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
CN4010	A4010B [O] A4010B [Y] A4010B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XC7Z020	* Power: DC * Interface/Protocol: 1G Ethernet, 1G TIM * Transceiver/Connector: RJ45
CN4020	A4020B [O] A4020B [Y] A4020B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XC7Z020	* Power: DC * Interface/Protocol: 1G Ethernet, 1G TIM * Transceiver/Connector: SFP
CN6010	A6010B [O] A6010B [Y] A6010B [T] A6011B [O] A6011B [Y] A6011B [T] A6012B [O] A6012B [Y] A6012B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XC7Z020	* Power: AC, DC, AC/DC * Interface/Protocol: 1G Ethernet, 1G TIM * Transceiver/Connector: RJ45, SFP
CN6100	A6100B [O] A6100B [Y] A6100B [T] A6101B [O] A6101B [Y] A6101B [T] A6102B [O] A6102B [Y] A6102B [T]	5.5.0/5.5.1	Intel® ATOM, Xilinx® XC6VLX195T	* Power: AC, DC, AC/DC * Interface/Protocol: 10G Ethernet, 10G TIM * Transceiver/Connector: XFP
CN6110	A6110B [O] A6110B [Y] A6110B [T] A6111B [O] A6111B [Y] A6111B [T] A6112B [O] A6112B [Y] A6112B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XC7Z030	* Power: AC, DC, AC/DC * Interface/Protocol: 1G Ethernet, 1G TIM, 10G Ethernet, 10G TIM * Transceiver/Connector: RJ45, SFP+
CN6140	A6140B [O] A6140B [Y] A6140B [T] A6141B [O] A6141B [Y] A6141B [T] A6142B [O] A6142B [Y] A6142B [T]	5.5.0/5.5.1	Arm® Cortex A9 Xilinx® XC7Z045	* Power: AC, DC, AC/DC * Interface/Protocol: 1G Ethernet, 1G TIM, 10G Ethernet, 10G TIM, 4x10G Ethernet * Transceiver/Connector: SFP+
CN9100	A9100B [O] A9100B [Y] A9100B [T] A9101B [O] A9101B [Y] A9101B [T] A9102B [O] A9102B [Y] A9102B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XCVU095	* Power: AC, DC, AC/DC * Interface/Protocol: 100G Ethernet * Transceiver/Connector: CFP4
CN9120	A9120B [O] A9120B [Y] A9120B [T] A9121B [O] A9121B [Y] A9121B [T] A9122B [O] A9122B [Y] A9122B [T]	5.5.0/5.5.1	Arm® Cortex A9, Xilinx® XCVU095	* Power: AC, DC, AC/DC * Interface/Protocol: 100G Ethernet * Transceiver/Connector: QSFP28

Table 2: Tested Module Identification – Hardware

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

2.3 Excluded Components

None

2.4 Modes of Operation

Modes List and Description:

The module supports an approved mode of operation. The module will be in the approved mode of operation when configured as detailed in section 11.2 Administrator Guidance. The Module does not implement any non-approved services when configured as per section 11.2 Administrator Guidance.

Mode Name	Description	Type	Status Indicator
FIPS mode	fips parameter on/enabled	Approved	CLI "fips" command, CM7 Status pane (FIPS Mode)

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

The module implements the approved algorithms in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3451	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3435	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3437	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3439	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3445	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3451	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CFB128	A3549	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CTR	A3435	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3436	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3437	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3438	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3439	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3440	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3441	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3442	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A3443	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3444	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3445	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3446	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3447	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3448	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3451	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3458	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3459	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3460	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3492	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3549	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Counter Tests Performed - Yes	SP 800-38A
AES-GCM	A3435	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	
AES-GCM	A3436	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3437	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3438	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3439	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3440	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3441	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A3442	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3443	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3444	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3445	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3446	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3447	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3448	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3451	Direction - Decrypt, Encrypt IV Generation - Internal	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		IV Generation Mode - 8.2.2 Key Length - 128, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 120, 128, 248, 256, 0 AAD Length - AAD Length: 0, 120, 128, 248, 256	
AES-GCM	A3458	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3459	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3460	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
AES-GCM	A3549	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 368, 384, 1016, 1024 AAD Length - AAD Length: 112, 128, 640, 688	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A3451	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A3451	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3451	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3451	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
Hash DRBG	A3451	Prediction Resistance - No Supports Reseed - No Mode - SHA2-256 Entropy Input - Entropy Input: 512 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-1024 Increment 8 Additional Input - Additional Input: 0-1024 Increment 8 Returned Bits - 1024	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA-1	A3451	MAC - MAC: 160 Key Length - Key Length: 80-320 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3450	MAC - MAC: 256 Key Length - Key Length: 80-320 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3451	MAC - MAC: 256 Key Length - Key Length: 80-320 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3451	MAC - MAC: 384 Key Length - Key Length: 80-320 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3451	MAC - MAC: 512 Key Length - Key Length: 80-320 Increment 8	FIPS 198-1
KAS-ECC Sp800-56Ar3	A3451	Domain Parameter Generation Methods - P-256, P-384, P-521 Function - Full Validation, Key Pair Generation iutId - 123456ABCD Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-256 Fixed Info Pattern - literal[abcd1234]||uPartyInfo||vPartyInfo Fixed Info Encoding - Concatenation Key Length - 256	SP 800-56A Rev. 3
KAS-FFC Sp800-56Ar3	A3451	Domain Parameter Generation Methods - MODP-2048 Function - Full Validation, Key Pair Generation iutId - 123456ABCD Scheme - dhEphem - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-256 Fixed Info Pattern - literal[abcd1234]||uPartyInfo||vPartyInfo Fixed Info Encoding - Concatenation Key Length - 256	SP 800-56A Rev. 3
KDF SNMP (CVL)	A3451	Password Length - Password Length: 64-232 Increment 8 Engine ID - 80000dce0300d01f010ce8, 80000dce0300d01f010ce9	SP 800-135 Rev. 1
KDF SP800-108	A3451	KDF Mode - Counter MAC Mode - HMAC-SHA2-256 Supported Lengths - Supported Lengths: 256 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SSH (CVL)	A3451	Cipher - AES-128, AES-256 Hash Algorithm - SHA2-256, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A3451	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KTS-IFC	A3451	Function - keyPairGen, partialVal IUT ID - CAFECAFE Modulo - 2048 Key Generation Methods - rsakpg1-basic Fixed Public Exponent - 010001 Scheme - KTS-OAEP-basic - KAS Role - initiator, responder Key Transport Method - Hash Algorithms - SHA2-256 Supports Null Associated Data - Yes Associated Data Encoding - concatenation Key Length - 256	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-4)	A3451	Key Generation Mode - B.3.6 Modulo - 2048 Primality Tests - Table C.3 Info Generated By Server - No Public Exponent Mode - Fixed Fixed Public Exponent - 010001 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3451	Signature Type - PKCS 1.5 Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256	FIPS 186-4
RSA SigVer (FIPS186-4)	A3451	Signature Type - PKCS 1.5 Modulo - 2048, 4096 Hash Pair - Hash Algorithm - SHA2-256 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
Safe Primes Key Generation	A3451	Safe Prime Groups - MODP-2048	SP 800-56A Rev. 3
Safe Primes Key Verification	A3451	Safe Prime Groups - MODP-2048	SP 800-56A Rev. 3
SHA-1	A3451	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A3450	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	A3451	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A3451	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3451	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-256	A3449	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
TDES-CFB8	A3451	Direction - Decrypt Keying Option - 1	SP 800-67 Rev. 2
TLS v1.2 KDF RFC7627 (CVL)	A3451	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Note 1: Triple-DES is only used to decrypt CSPs stored in FLASH memory 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: The module does not generate RSA keys < 2048 for use in X.509v3 certificates in accordance with SP 800-131Arev2.
Note 3: The module does not support the use of SHA-1 for X.509v3 certificate digital signatures in line with SP 800-131Arev2.
Note 4: 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 5: 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 6: 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 7: 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 8: 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.

Vendor-Affirmed Algorithms:

The module implements the vendor-affirmed algorithms in the table below.

Name	Properties	Implementation	Reference
CKG 1	Key Type:Symmetric and Asymmetric	N/A	SP 800-133rev2 Section 4/Example 1
CKG 2	Key Type:Symmetric	N/A	SP 800-133rev2 Section 6.3/ Approved Method 2

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

The module implements the security functions listed in the table below.

Name	Type	Description	Properties	Algorithms
Symmetric Encryption/Decryption SMK	BC-UnAuth			AES-CFB128: (A3451) Key Length: 256
Symmetric Decryption SMK	BC-UnAuth			TDES-CFB8: (A3451)
Symmetric Encryption/Decryption Data Plane 1	BC-Auth BC-UnAuth	1G Ethernet FPGA Bulk encryption/ decryption of User data.		AES-CFB128: (A3435, A3437, A3439, A3445, A3549) AES-CTR: (A3435, A3437, A3439, A3445, A3451, A3549) AES-GCM: (A3435, A3437, A3439, A3445, A3549)
Symmetric Encryption/Decryption Data Plane 2	BC-Auth BC-UnAuth	1G Ethernet TIM FPGA Bulk encryption/ decryption of User data.		AES-CTR: (A3436, A3438, A3440, A3443, A3460) AES-GCM: (A3436, A3438, A3440, A3443, A3460)

Name	Type	Description	Properties	Algorithms
Symmetric Encryption/Decryption Data Plane 3	BC-Auth BC-UnAuth	10G Ethernet FPGA Bulk encryption/ decryption of User data.		AES-CTR: (A3459, A3441, A3448) AES-GCM: (A3459, A3441, A3448)
Symmetric Encryption/Decryption Data Plane 4	BC-Auth BC-UnAuth	10G Ethernet TIM FPGA Bulk encryption/ decryption of User data.		AES-CTR: (A3458, A3442, A3444) AES-GCM: (A3458, A3442, A3444)
Symmetric Encryption/Decryption Data Plane 5	BC-UnAuth	10Gx4 Ethernet FPGA Bulk encryption/ decryption of User data.		AES-CTR: (A3492)
Symmetric Encryption/Decryption Data Plane 6	BC-Auth BC-UnAuth	100G Ethernet FPGA Bulk encryption/ decryption of User data.		AES-CTR: (A3446, A3447) AES-GCM: (A3446, A3447)
Symmetric Encryption/Decryption TLS	BC-Auth BC-UnAuth	Encryption/ decryption of TLS session data		AES-CBC: (A3451) AES-GCM: (A3451)
Symmetric Encryption/Decryption SSH	BC-UnAuth	Encryption/ decryption of SSH session data		AES-CTR: (A3451)
Symmetric Encryption/Decryption SNMPv3	BC-UnAuth	Encryption/ decryption of SNMPv3 session data		AES-CFB128: (A3451)
KAS SME	KAS-Full	SME Key Agreement between modules	IG D.F:Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC Sp800-56Ar3: (A3451)
KAS TLS	KAS-Full	TLSv1.2 Key Agreement	IG D.F:Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC Sp800-56Ar3: (A3451)
KAS SSH	KAS-Full	SSH Key Agreement	IG D.F:Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC Sp800-56Ar3: (A3451)
KAS SNMP	KAS-Full	SNMP Key Agreement	IG D.F:Scenario 2 path (2) Bit Strength Caveat:provides 112 bits of encryption strength	KAS-FFC Sp800-56Ar3: (A3451)
KTS 1	KTS-Encap	Key Transport between modules	IG D.G:Approved Method, Bullet 2 Bit Strength Caveat:provides 112 bits of encryption strength	KTS-IFC: (A3451) SHA2-256: (A3451)

Name	Type	Description	Properties	Algorithms
KTS 2	KTS-Wrap	SME Key Transport between modules	IG D.G:Approved Method, Bullet 1 Bit Strength Caveat:provides 256 bits of encryption strength	AES-CFB128: (A3451) Key Length: 256 HMAC-SHA2-256: (A3451) SHA2-256: (A3451)
Authentication SME 1	DigSig-SigGen DigSig-SigVer	Authenticate remote end		RSA SigGen (FIPS186-4): (A3451) RSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451)
Authentication SME 2	DigSig-SigGen DigSig-SigVer	Authenticate remote end		ECDSA SigGen (FIPS186-4): (A3451) ECDSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451) SHA2-384: (A3451) SHA2-512: (A3451)
Authentication TLS 1	DigSig-SigGen DigSig-SigVer	Authenticate remote end		RSA SigGen (FIPS186-4): (A3451) RSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451)
Authentication TLS 2	DigSig-SigGen DigSig-SigVer	Authenticate remote end		ECDSA SigGen (FIPS186-4): (A3451) ECDSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451) SHA2-384: (A3451) SHA2-512: (A3451)
Authentication SSH	DigSig-SigGen DigSig-SigVer	Authenticate remote end		ECDSA SigGen (FIPS186-4): (A3451) ECDSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451) SHA2-384: (A3451) SHA2-512: (A3451)
Message Authentication TLS	MAC	Generation and verification of TLS data integrity		HMAC-SHA2-256: (A3451) HMAC-SHA2-384: (A3451) SHA2-256: (A3451) SHA2-384: (A3451)
Message Authentication SSH	MAC	Generation and verification of SSH data integrity		HMAC-SHA-1: (A3451) HMAC-SHA2-256: (A3451) HMAC-SHA2-512: (A3451) SHA-1: (A3451) SHA2-256: (A3451) SHA2-512: (A3451)
Message Authentication SNMP	MAC	Generation and verification of SNMP data integrity		HMAC-SHA-1: (A3451) HMAC-SHA2-512: (A3451) SHA-1: (A3451) SHA2-512: (A3451)

Name	Type	Description	Properties	Algorithms
KDF SME	KBKDF	Generate SME KEK and SME HMAC keys from KDK, Generate SME GEK and SME HMAC keys from GDK		KDF SP800-108: (A3451) HMAC-SHA2-256: (A3451) SHA2-256: (A3451)
KDF TIM	KBKDF	Generate TIM DEK from KDK		KDF SP800-108: (A3451) HMAC-SHA2-256: (A3451) SHA2-256: (A3451)
KDF TLS	KAS-135KDF			KDF TLS: (A3451) TLS v1.2 KDF RFC7627: (A3451) SHA2-256: (A3451) SHA2-384: (A3451)
KDF SSH	KAS-135KDF			KDF SSH: (A3451) SHA2-256: (A3451) SHA2-512: (A3451)
KDF SNMP	KAS-135KDF			KDF SNMP: (A3451) SHA-1: (A3451) SHA2-256: (A3451)
Secure Hash	SHA	Calculate secure hash		SHA2-256: (A3451)
DRBG Request	DRBG	Request random data from DRBG		Hash DRBG: (A3451) SHA2-256: (A3451)
Entropy Source	ENT-Cond ENT-ESV	Request Entropy		HMAC-SHA2-256: (A3450) SHA2-256: (A3450) SHA3-256: (A3449)
Firmware Load Test	DigSig-SigVer	Verify Firmware signature		RSA SigVer (FIPS186-4): (A3451) SHA2-256: (A3451)
Bypass Integrity Test	SHA	Check bypass parameter integrity		SHA2-256: (A3451)
Generate Asymmetric Keys 1 (RSA)	AsymKeyPair-KeyGen	Generate an asymmetric key pair	SP 800-133rev2 Sections 5.1:Asymmetric key generation using unmodified DRBG output	RSA KeyGen (FIPS186-4): (A3451) Hash DRBG: (A3451)
Generate Asymmetric Keys 2 (EC)	AsymKeyPair-KeyGen	Generate an asymmetric key pair	SP 800-133rev2 Sections 5.1 and 5.2:Asymmetric key generation using unmodified DRBG output	ECDSA KeyGen (FIPS186-4): (A3451) ECDSA KeyVer (FIPS186-4): (A3451) Hash DRBG: (A3451)
Generate Asymmetric Keys 3 (DH Key Generation during Key Agreement)	AsymKeyPair-KeyGen	Generate an asymmetric key pair	SP 800-133rev2 Sections 5.2:Asymmetric key generation using unmodified DRBG output	Safe Primes Key Generation: (A3451) Safe Primes Key Verification: (A3451) Hash DRBG: (A3451)
Generate Symmetric Key 1 (Direct generation from DRBG)	CKG	Generate a symmetric key	SP 800-133rev2 Section 6.1:Direct generation of symmetric key using unmodified DRBG output	CKG 1: ()

Name	Type	Description	Properties	Algorithms
Generate Symmetric Key 2 (Symmetric Keys Produced by Combining (Multiple) Keys and Other Data)	CKG	Generate a symmetric key	SP 800-133rev2 Section 6.3:Symmetric Keys Produced by Combining (Multiple) Keys and Other Data	CKG 2: ()
Sign X.509 Certificate	DigSig-SigGen	Sign an X.509 Certificate Signing Request		RSA SigGen (FIPS186-4): (A3451) ECDSA SigGen (FIPS186-4): (A3451) SHA2-256: (A3451) SHA2-384: (A3451) SHA2-512: (A3451)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM Key and IV generation for TLS (Conforms to FIPS 140-3 IG C.H/Scenario 1)

- 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.

AES-GCM Key and IV generation for data-plane encryption (Conforms to FIPS 140-3 IG C.H/Scenario 4)

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

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 below.

Algorithm Type	Algorithm
Authentication	RSA[2] ECDSA[1]
Key Exchange	ECDH[1] RSA-OAEP AES-256-CFB with HMAC-SHA256
Hash for HMAC	SHA-256
ECDH KDF	SHA-256 SHA-384 SHA-512
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

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 below.

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.

TLS Cryptographic Algorithms (KMS)

OpenSSL1 Cipher Suite	Authentication	Key Exchange	Symmetric Encryption	Hash for HMAC2
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.

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 below.

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.

SNMPv3 Protocol Algorithms

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

Algorithm Type	Algorithm
Authentication	HMAC-SHA1 HMAC-SHA512
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.

2.8 RBG and Entropy

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.

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.

Cert Number	Vendor Name
E51	Senetas Corporation Ltd, distributed by Thales SA (SafeNet)
E49	Senetas Corporation Ltd, distributed by Thales SA (SafeNet)

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Senetas TRNG Entropy Source	Physical	Xilinx® XC7Z015, Xilinx® XC7Z020, Xilinx® XC7Z030, Xilinx® XC7Z045	256 bits	Full Entropy	HMAC-SHA2-256 (A3450)
Senetas CPU Jitter Entropy Source	Non-Physical	Intel® Atom	256 bits	Full Entropy	SHA3-256 (A3449)

Table 8: Entropy Sources

2.9 Key Generation

Asymmetric RSA and ECDSA keys are generated in accordance with FIPS186-4. Symmetric keys are generated using unmodified DRBG output in accordance with SP 800-133rev2 or using the SP 800-108rev1 and the SP 800-135rev1 compliant KDF functions.

2.10 Key Establishment

Keys are established using KTS-IFC (RSA-OAEP-256) key transport process in accordance with SP 800-56Brev2, ECDH and DH ephemeral key agreement in accordance with SP 800-56Arev3.

2.11 Industry Protocols

The module supports TLSv1.2, SSH version 2.0 and SNMPv3.

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

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

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
RJ45 Management Ethernet	Control Input Status Output	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	CLI
USB	Control Input	Upgrade image transfer
Keypad	Control Input	Navigation of LCD menu system and limited configuration input (Set IP address, Activation via CM7, USB upgrades)
LCD	Status Output	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	Indicate powered state
System LED	Status Output	Indicate the system operational state
Secure LED	Status Output	Indicate the system secure state
LAN LED	Status Output	Indicate management LAN link status and activity
Local LED	Status Output	Indicate Local Port link status and activity
Network LED	Status Output	Indicate Network Port link status and activity
Alarm LED	Status Output	Indicate system alarm state
Temperature LED	Status Output	Indicate temperature warning alarm
Battery LED	Status Output	Indicate internal battery state
Network Port	Data Input Data Output Status Output	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	Data Input Data Output	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	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	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

Table 9: Ports and Interfaces

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

CN4010 Ports

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

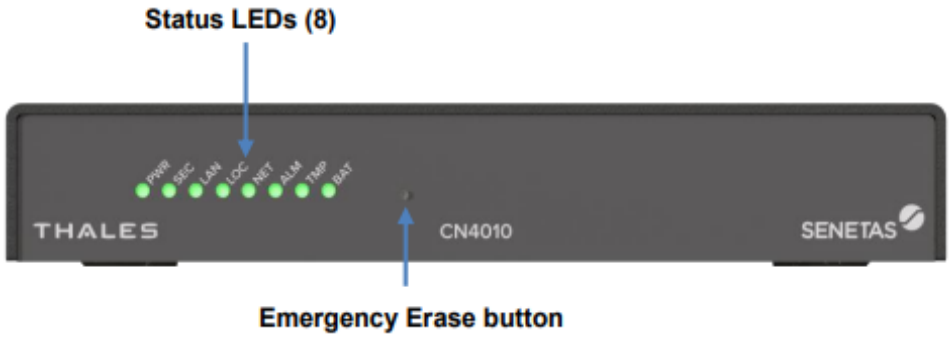

Figure 9 – Front View of the CN4010 Encryptor

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.

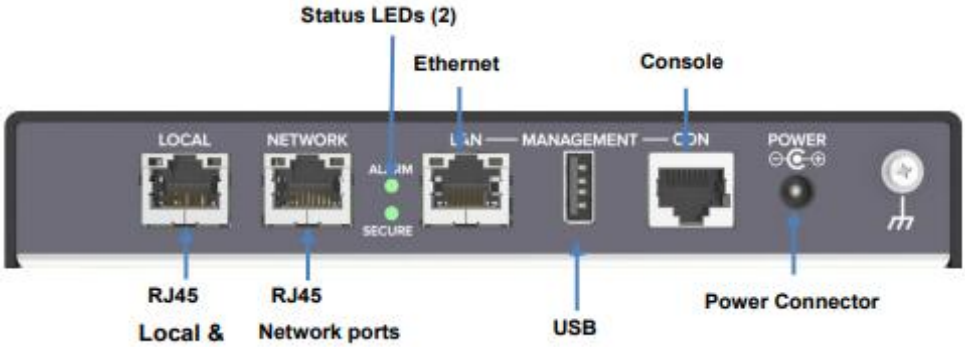

Figure 10 – Rear View of the CN4010 Encryptor

CN4020 Ports

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

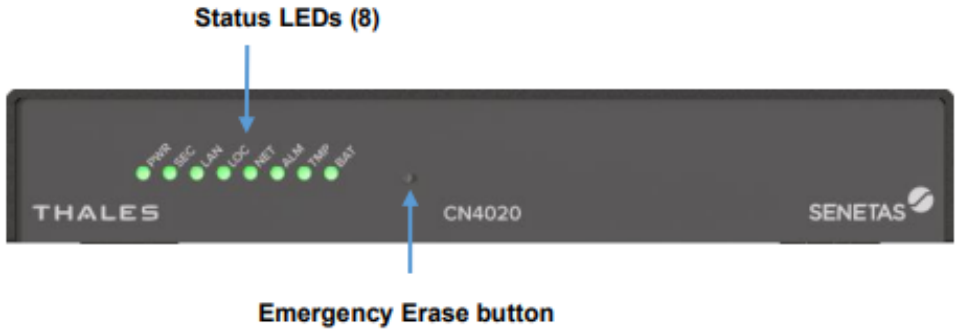

Figure 11 – Front View of the CN4020 Encryptor

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.

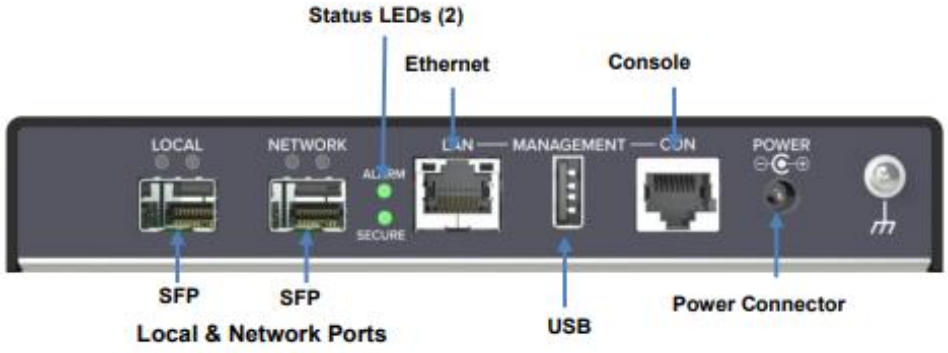

Figure 12 – Rear View of the CN4020 Encryptor

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.

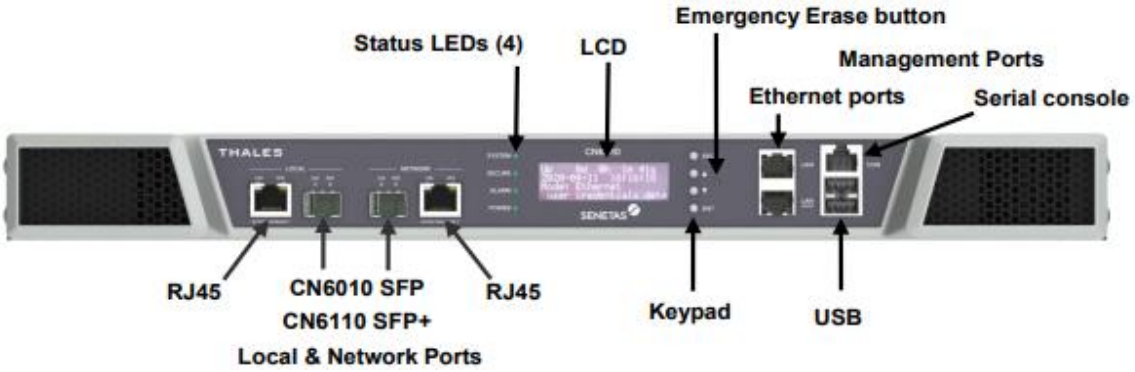

Figure 13 – Front View of the CN6010 & CN6110 Encryptor

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.

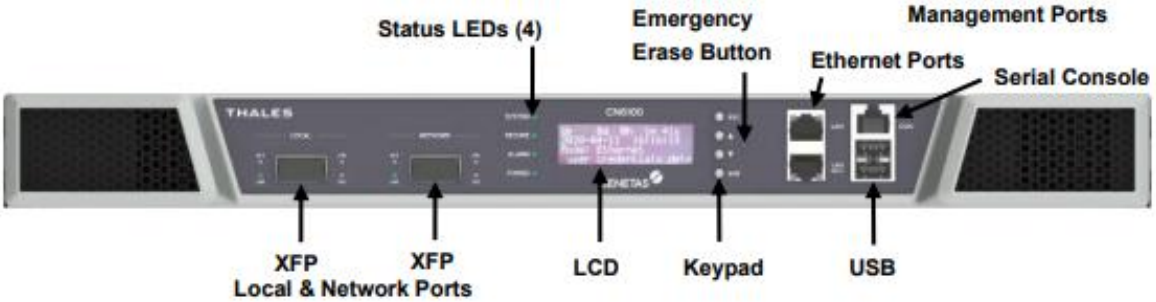

Figure 14 – Front View of the CN6100 Encryptor

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.

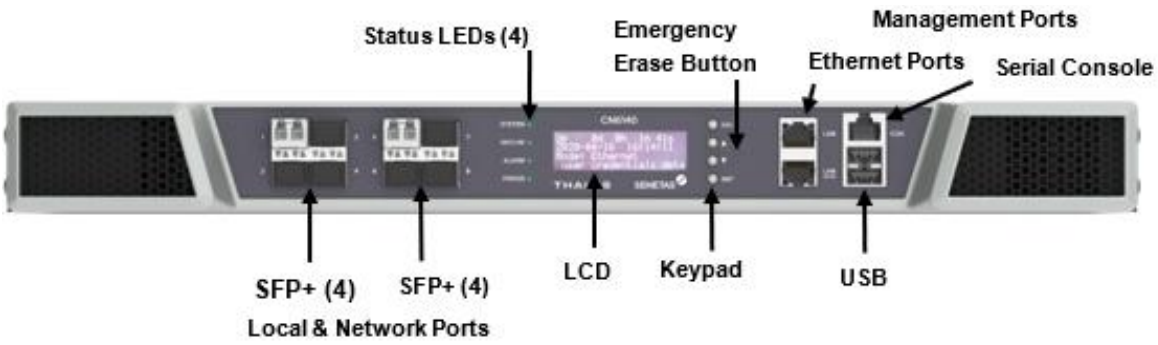

Figure 15 – Front View of the CN6140 Encryptor

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.

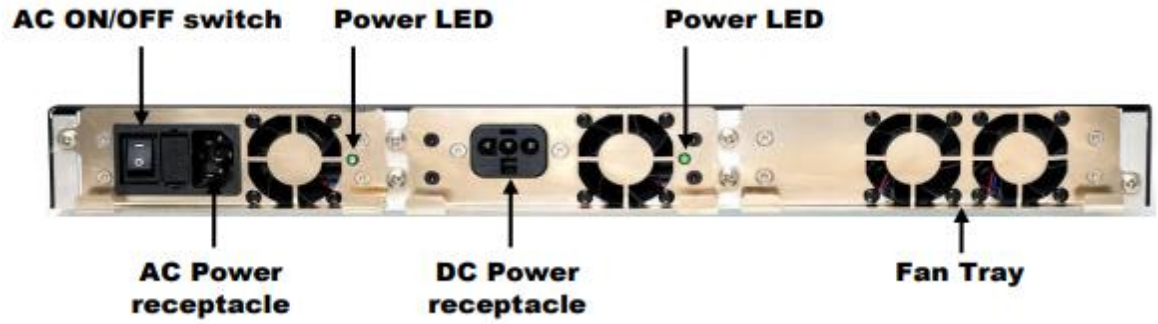

Figure 16 – Rear View: CN6000 Series Encryptor

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.

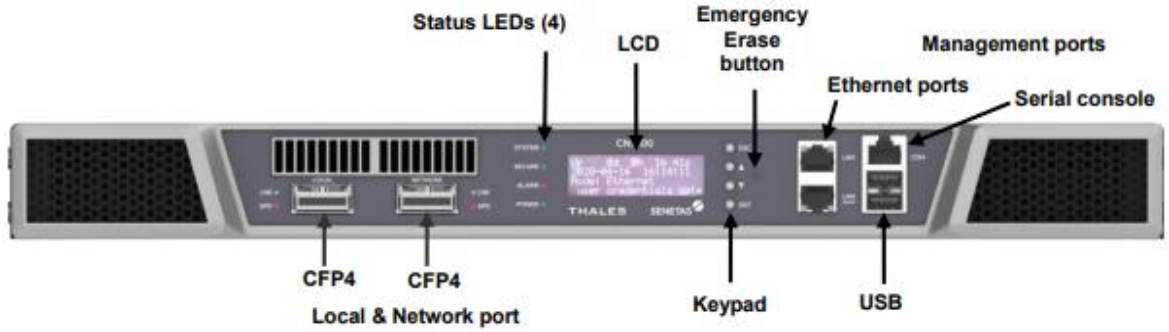

Figure 17 – Front View of the CN9100 Encryptor

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.

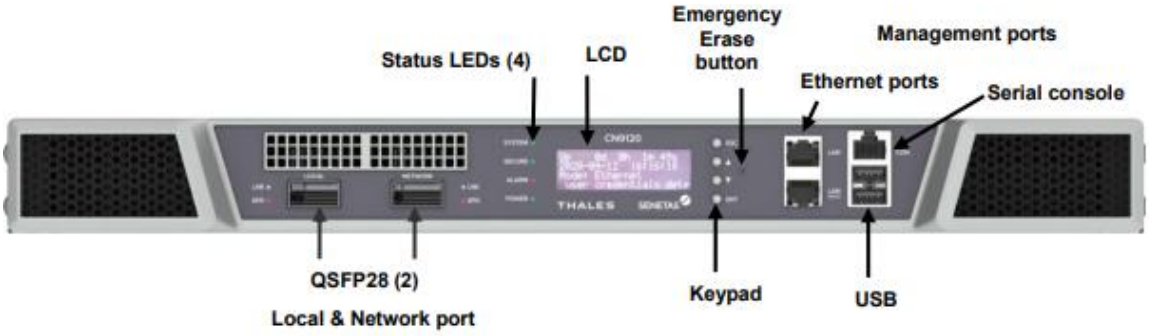

Figure 18 – Front View of the CN9120 Encryptor

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.

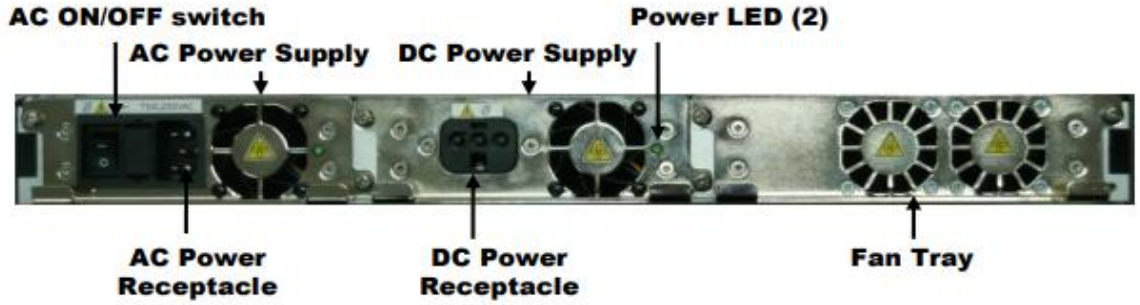

Figure 19 – Rear View: CN9000 Series Encryptor

3.2 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 zeroisation of data plane cryptographic keys and SSP zeroisation occurs when the tamper circuit is triggered. During the upgrade process the module inhibits data when loading the new software image until the self-tests have completed successfully. In addition, the system's underlying operational environment logically separates key management functions and SSP data from the data plane. All input and output of data on the management plane and data plane are either physically separated (separate ports) or logically separated by protocol type.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The supported authentication methods are listed in the table below.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Console Auth	Direct console CLI connection	Username and Password	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, 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.
SSH Auth	Remote SSH CLI connection	Username and Password	Crypto Officers and Users accessing the module CLI, via Remote SSH CLI, 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, 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.
SNMP Auth	Remote SNMP connection	Username and Password	Crypto Officers and Users accessing the module via SNMPv3, 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	User passwords must be at least 8 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. Assuming an automated brute force attack that can make 20 login attempts per second then the probability of success in one minute is 1200/94^8 which is less than 1/100,000.
HTTPS Auth	Remote connection to Restful interface	Username and Password	Crypto Officers and Users accessing the module via the Restful interface, 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	User passwords must be at least 8 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. Assuming an automated brute force attack that can make 20 login attempts per second then the probability of success in one minute is 1200/94^8 which is less than 1/100,000.

Table 10: Authentication Methods

Note: The module suppresses feedback of authentication data being entered, by returning * or blank characters.

4.2 Roles

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.

The module's access control rules, system timing, and internal controls maintain separation of the multiple concurrent operators. Only 10 concurrent users can access the CLI via SSH.

The module supports four user roles as detailed in the table below.

Name	Type	Operator Type	Authentication Methods
Administrator	Identity	CO	Console Auth SSH Auth SNMP Auth HTTPS Auth
Supervisor	Identity	CO	Console Auth SSH Auth SNMP Auth HTTPS Auth
Upgrader	Identity	CO	Console Auth SSH Auth SNMP Auth HTTPS Auth
Operator	Identity	User	Console Auth SSH Auth SNMP Auth HTTPS Auth

Table 11: Roles

4.3 Approved Services

The module supports the approved services listed in the table below.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set Real Time Clock		N/A	Time and Date	New time and date		Administrator Supervisor
Activation	Activate an erased module by updating the primary administrator account credentials.	activation status, audit log	New administrator credentials	Status	Symmetric Encryption/Decryption SMK KTS 1 Secure Hash	Administrator - Activation RSA Private Key: E - Activation RSA Public Key: R - Authentication Passwords: W - Authentication Password Hash: G - System Master Key (SMK): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Generate X.509v3 Certificate Signing Request	Generate an X.509v3 certificate signing request to be signed by a trusted certifying authority	certificate status, audit log	Certificate Details	CSR	Symmetric Encryption/Decryption SMK Generate Asymmetric Keys 1 (RSA) Generate Asymmetric Keys 2 (EC)	Administrator - RSA Private Keys: G - RSA Public Keys: G - ECDSA Private Keys: G - ECDSA Public Keys: G - X509v3 Certificates: R - System Master Key (SMK): E
Load X.509v3 Certificate (*Note 1)	Load a signed X.509 Certificate	certificate status audit log	Signed X.509 Certificate	Updated certificate table		Administrator - RSA Public Keys: W - ECDSA Public Keys: W - X509v3 Certificates: W
Create User Account		command status, audit log	User details and passwords	Updated user table	Symmetric Encryption/Decryption SMK Secure Hash	Administrator - Authentication Passwords: W - Authentication Password Hash: G - System Master Key (SMK): E
Modify User Account		command status, audit log	User details and passwords	Updated user record	Symmetric Encryption/Decryption SMK Secure Hash	Administrator - Authentication Passwords: W - Authentication Password Hash: G - System Master Key (SMK): E
Delete User Account		command status, audit log	User record index	Updated user table		Administrator - Authentication Passwords: Z - Authentication Password Hash: Z
View User Account		N/A	User record index	User record		Administrator
Edit Connection Action Table (Bypass)		command status, audit log	Command	Connection status	Bypass Integrity Test	Administrator Supervisor
View Connection Action Table		N/A	Command	Connection table		Administrator Supervisor Upgrader Operator
Show Version		N/A	Command	Versioning info		Administrator Supervisor Upgrader Operator

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status		N/A	Command	Status information		Administrator Supervisor Upgrader Operator
Clear Audit Trail		N/A	Command	Command status		Administrator
View Audit Trail		N/A	Command	Audit log		Administrator Supervisor Upgrader Operator
Clear Event Log		N/A	Command	Command status		Administrator
View Event Log		N/A	Command	Event log		Administrator Supervisor Upgrader Operator
Change FIPS mode status		command status, audit log	FIPS mode setting (on/off)	Command status		Administrator
Run Self-test (Reboot Command)		N/A	Command	Self-test status		Administrator Supervisor
Install Firmware Upgrade		command status, audit log	Signed firmware upgrade image	Updated firmware version	Symmetric Decryption SMK Firmware Load Test	Administrator - Firmware Upgrade RSA Public Key: E - Triple-DES System Master Key: E Upgrader - Firmware Upgrade RSA Public Key: E - Triple-DES System Master Key: E
Establish FTPS (TLS) Session		command status, event log	Session parameters	Connection success/failure	Symmetric Encryption/Decryption SMK Symmetric Encryption/Decryption TLS KAS TLS Authentication TLS 2 Message Authentication TLS KDF TLS Generate Asymmetric Keys 2 (EC)	Administrator - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificates: R,W - System Master Key (SMK): E Upgrader - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: R,W - System Master Key (SMK): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Establish SFTP (SSH) Session		command status, event log	Session parameters	Connection success/failure	Symmetric Encryption/Decryption SMK Symmetric Encryption/Decryption SSH KAS SSH Authentication SSH Message Authentication SSH KDF SSH Generate Asymmetric Keys 2 (EC)	Administrator - SSH Private Keys: E - SSH Public Keys: R,E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E - System Master Key (SMK): E Upgrader - SSH Private Keys: E - SSH Public Keys: R,E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E - System Master Key (SMK): E
Re/Start Secure Connection	Start or restart a data plane secure connection	command status, event log	Command	Connection success/failure	Symmetric Encryption/Decryption SMK Symmetric Encryption/Decryption Data Plane 1 Symmetric Encryption/Decryption Data Plane 2 Symmetric Encryption/Decryption Data Plane 3 Symmetric Encryption/Decryption Data Plane 4 Symmetric Encryption/Decryption Data Plane 5 Symmetric Encryption/Decryption Data Plane 6 KAS SME KTS 1 KTS 2	Administrator - RSA Private Keys: E - RSA Public Keys: R,W,E - ECDSA Private Keys: E - ECDSA Public Keys: R,W,E - SME ECDH Private Keys: G,E - SME ECDH Public Keys: G,R,W,E - SME ECDH Shared Secret: G,E - SME KDK: G,R,W,E - Group Derivation Keys (GDK): G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Authentication SME 1 Authentication SME 2 KDF SME KDF TIM Generate Asymmetric Keys 2 (EC) Generate Symmetric Key 1 (Direct generation from DRBG)	- Key Encrypting Keys (KEK): G,E - Group Establishment Keys (GEK): G,E - SME HMAC keys: G,E - Data Encrypting Keys (DEK): G,R,W,E - TIM KDK: E - X509v3 Certificates: R,W - System Master Key (SMK): E Supervisor - RSA Private Keys: E - RSA Public Keys: R,W,E - ECDSA Private Keys: E - ECDSA Public Keys: R,W,E - SME ECDH Private Keys: G,E - SME ECDH Public Keys: G,R,W,E - SME ECDH Shared Secret: G,E - SME KDK: G,R,W,E - Group Derivation Keys (GDK): G,E - Key Encrypting Keys (KEK): G,E - Group Establishment Keys (GEK): G,E - SME HMAC keys: G,E - Data Encrypting Keys (DEK): G,R,W,E - TIM KDK: E - X509v3 Certificates: R,W - System Master Key (SMK): E

Erase Module - Zeroise (CLI Command)	Zeroise Module	command status, event log	Command	Status	None	Administrator - System Master Key (SMK): Z - Triple-DES System Master Key: Z - SMK_Local: Z - SMK_Mask: Z - SMK_CSP: Z - Activation RSA Private Key: Z - Activation RSA Public Key: Z - RSA Private Keys: Z - RSA Public Keys: Z - ECDSA Private Keys: Z - ECDSA Public Keys: Z - SME ECDH Private Keys: Z - SME ECDH Public Keys: Z - SME ECDH Shared Secret: Z - X509v3 Certificates: Z - Authentication Passwords: Z - Authentication Password Hash: Z - Key Encrypting Keys (KEK): Z - Data Encrypting Keys (DEK): Z - TIM KDK: Z - Group Establishment Keys (GEK): Z - SME HMAC keys: Z - SME KDK: Z - Group Derivation Keys (GDK): Z - SNMPv3 Diffie Hellman Private Keys: Z - SNMPv3 Diffie Hellman Public Keys: Z - SNMPv3 Diffie Hellman Shared Secret: Z - SNMPv3 Privacy Keys: Z - SNMPv3 Integrity Keys: Z - DRBG Seed: Z - DRBG Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Input and Nonce: Z - DRBG V and C internal state parameters: Z - SSH Private Keys: Z - SSH Public Keys: Z - SSH Key Exchange Private Keys: Z - SSH Key Exchange Public Keys: Z - SSH Shared Secret: Z - SSH Privacy Keys: Z - SSH Integrity Keys: Z - TLS Private Keys: Z - TLS Public Keys: Z - TLS Key Exchange Private Keys: Z - TLS Key Exchange Public Keys: Z - TLS Premaster Secrets: Z - TLS Master Secrets: Z - TLS Privacy Keys: Z - TLS Integrity Keys: Z - Keyvault Private Keys: Z - Keyvault Public Keys: Z - Firmware Upgrade RSA Public Key: Z
Establish a Remote Management (SNMP) Session		Login status	Session parameters	Connection success/failure	Symmetric Encryption/Decryption SNMPv3 KAS SNMP Message Authentication SNMP KDF SNMP Generate Asymmetric Keys 3 (DH Key Generation during Key Agreement)	Administrator - SNMPv3 Diffie Hellman Private Keys: G,E - SNMPv3 Diffie Hellman Public Keys: G,R,E - SNMPv3 Diffie Hellman Shared Secret: G,E - SNMPv3 Privacy Keys: G,E - SNMPv3 Integrity Keys: G,E Supervisor

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SNMPv3 Diffie Hellman Private Keys: G,E - SNMPv3 Diffie Hellman Public Keys: G,R,E - SNMPv3 Diffie Hellman Shared Secret: G,E - SNMPv3 Privacy Keys: G,E - SNMPv3 Integrity Keys: G,E Upgrader - SNMPv3 Diffie Hellman Private Keys: G,E - SNMPv3 Diffie Hellman Public Keys: G,R,E - SNMPv3 Diffie Hellman Shared Secret: G,E - SNMPv3 Privacy Keys: G,E - SNMPv3 Integrity Keys: G,E Operator - SNMPv3 Diffie Hellman Private Keys: G,E - SNMPv3 Diffie Hellman Public Keys: G,R,E - SNMPv3 Diffie Hellman Shared Secret: G,E - SNMPv3 Privacy Keys: G,E - SNMPv3 Integrity Keys: G,E

Establish a Remote CLI (SSH) Session	Login status	Session parameters	Connection success/failure	Symmetric Encryption/Decryption SSH KAS SSH Authentication SSH Message Authentication SSH KDF SSH Generate Asymmetric Keys 2 (EC)	Administrator - SSH Public Keys: E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E Supervisor - SSH Public Keys: E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E Upgrader - SSH Public Keys: E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E Operator - SSH Public Keys: E - SSH Key Exchange Private Keys: G,E - SSH Key Exchange Public Keys: G,R,E - SSH Shared Secret: G,E - SSH Privacy Keys: G,E - SSH Integrity Keys: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Establish RESTful HTTPS (TLS) Session		HTTPS Connection status	Session parameters	Connection success/failure	Symmetric Encryption/Decryption SMK Symmetric Encryption/Decryption TLS KAS TLS Authentication TLS 2 Message Authentication TLS KDF TLS Generate Asymmetric Keys 2 (EC)	Administrator - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: R - System Master Key (SMK): E Supervisor - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: R - System Master Key (SMK): E Upgrader - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: R - System Master Key (SMK): E Operator - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: R - System Master Key (SMK): E
KeyVault Sign (X.509v3 Certificate Signing Request)	Sign an X.509v3 CSR	operation output	CSR for signing	Signed certificate	Symmetric Encryption/Decryption SMK Sign X.509 Certificate	Administrator - RSA Private Keys: E - ECDSA Private Keys: E - X509v3 Certificates: R,W - System Master Key (SMK): E
KeyVault Encrypt	Encrypt a base64url encoded 32 byte block of plaintext.	operation output	32 Byte plaintext data block	Encrypted block	KTS 1	Administrator - RSA Public Keys: E
KeyVault Decrypt	Decrypt a base64url encoded 32 byte block of ciphertext	operation output	32 Byte encrypted data block	Decrypted block	Symmetric Encryption/Decryption SMK KTS 1	Administrator - RSA Private Keys: E - System Master Key (SMK): E
KeyVault DRBG Access	Output a 32 byte block of random data from the DRBG	operation output	Command	32 byte output from DRBG	DRBG Request	Administrator - DRBG Entropy Input and Nonce: E - DRBG Seed: E - DRBG V and C internal state parameters: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
KeyVault Backup	Create backup of CA certificate	operation output	Command	Backup file	Symmetric Encryption/Decryption SMK	Administrator - Keyvault Private Keys: R,E - Keyvault Public Keys: R,E - System Master Key (SMK): E
KeyVault Restore	Restore backup of CA certificate	operation output	Command, Backup file	Command status	Symmetric Encryption/Decryption SMK	Administrator - Keyvault Private Keys: W,E - Keyvault Public Keys: W,E - System Master Key (SMK): E
Enable KeySecure	Enable KeySecure connector	operation output, audit log	Command	Command status	Symmetric Encryption/Decryption SMK Symmetric Encryption/Decryption TLS KAS TLS Authentication TLS 1 Authentication TLS 2 Message Authentication TLS KDF TLS Generate Asymmetric Keys 2 (EC) Generate Symmetric Key 1 (Direct generation from DRBG) Generate Symmetric Key 2 (Symmetric Keys Produced by Combining (Multiple) Keys and Other Data)	Administrator - TLS Private Keys: E - TLS Public Keys: R,E - TLS Key Exchange Private Keys: G,E - TLS Key Exchange Public Keys: G,R,E - TLS Premaster Secrets: G,E - TLS Master Secrets: G,E - TLS Privacy Keys: G,E - TLS Integrity Keys: G,E - X509v3 Certificates: W - SMK_Local: G,E - SMK_Mask: W,E - SMK_CSP: G,E - System Master Key (SMK): E
Generate Random		command status, audit log	Command	Random	DRBG Request Entropy Source	Administrator - DRBG Entropy Input and Nonce: E - DRBG Seed: E - DRBG V and C internal state parameters: E

Table 12: Approved Services

Note 1: 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.

The abbreviations of the access rights to SSPs have the following interpretation:

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.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

Only signed and authenticated firmware upgrade images that pass the firmware load test can be installed on the module by authorised users.

4.6 Bypass Actions and Status

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 status is evident through policy configuration.

5 Software/Firmware Security

5.1 Integrity Techniques

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-test, 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 Self-Tests for further information.

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

N/A. 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.

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	In accordance with the organization's Security Policy.	Tamper indication is available to all user roles via 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.

Table 13: Mechanisms and Actions Required

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 metal 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 zeroisation of all SSPs. For further details refer to Section 9.3 SSP Zeroization Methods.
3. Two tamper evident seals are pre-installed (at factory). Both are placed between the top cover and underside of the main enclosure. 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 20 – CN4000 Series factory installed tamper seals

Figure 21 – CN6000 Series factory installed tamper seals

Figure 22 – CN9000 Series factory installed tamper seals

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

7.2 EFP/EFT Information

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 the table below.

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	CN4010: 15 C, CN4020: 15 C, CN6010: 20 C, CN6100: 5 C, CN6110/CN6140: 10 C, CN9100/CN9120: 10 C	EFP	Shutdown
HighTemperature	CN4010: 85 C, CN4020: 80 C, CN6010: 85 C, CN6100: 80C, CN6110/CN6140: 80 C, CN9100/CN9120: 85C	EFP	Shutdown
LowVoltage	CN4010: 9.0 V, CN4020/CN6010/CN6100/CN6110/CN6140/CN9100/CN9120: 10.2 V	EFP	Shutdown
HighVoltage	CN4010: 15.0 V, CN4020/CN6010/CN6100/CN6110/CN6140/CN9100/CN9120: 13.8 V	EFP	Shutdown

Table 14: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

The module's enclosures were tested across the temperature ranges detailed in the table below. No perceptible deformation or change to the enclosure's integrity occurred during testing.

Temperature Type	Temperature
LowTemperature	-20 C
HighTemperature	80 C

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The module's SSP storage areas are detailed in the table below.

Storage Area Name	Description	Persistence Type
FLASH Memory	Storage of encrypted CSPs and PSPs in FLASH file system.	Static
SDRAM	Temporary storage of SSPs in main dynamic memory.	Dynamic
BBRAM	Tamper protected battery backed dynamic memory used for storage of the SMK. A tamper event will erase the contents of the BBRAM whether the module is in a powered or unpowered state.	Static
High Speed Crypto System	Storage of data plane connection DEKs in FPGA memory blocks.	Dynamic

Table 16: Storage Areas

9.2 SSP Input-Output Methods

The module's SSP input-output methods are detailed in the table below.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Keysecure Input	KeySecure Key Server	SDRAM	Encrypted	Manual	Electronic	
Activation Public Key Output	FLASH Memory	CM7	Encrypted	Manual	Electronic	
Keyvault Backup	FLASH Memory	CM7	Encrypted	Manual	Electronic	
Keyvault Restore	CM7	FLASH Memory	Encrypted	Manual	Electronic	
SME Public Key Input 1	Peer encryptor	SDRAM	Plaintext	Automated	Electronic	
SME Public Key Output 1	FLASH Memory	Peer encryptor	Plaintext	Automated	Electronic	
SME Public Key Input 2	Peer encryptor	SDRAM	Plaintext	Automated	Electronic	KAS SME
SME Public Key Output 2	SDRAM	Peer encryptor	Plaintext	Automated	Electronic	KAS SME
X509v3 Certificate Input 1	CM7	FLASH Memory	Encrypted	Manual	Electronic	
X509v3 Certificate Input 2	SSH CLI	FLASH Memory	Encrypted	Manual	Electronic	
X509v3 Certificate Input 3	CLI	FLASH Memory	Plaintext	Manual	Electronic	
X509v3 Certificate Input 4	Peer encryptor via SME	SDRAM	Plaintext	Automated	Electronic	
X509v3 Certificate Input 5	TLS Server	SDRAM	Plaintext	Automated	Electronic	
X509v3 Certificate Output 1	FLASH Memory	CM7	Encrypted	Manual	Electronic	
X509v3 Certificate Output 2	FLASH Memory	SSH CLI	Encrypted	Manual	Electronic	
X509v3 Certificate Output 3	FLASH Memory	CLI	Plaintext	Manual	Electronic	
X509v3 Certificate Output 4	FLASH Memory	Peer Encryptor via SME	Plaintext	Automated	Electronic	
X509v3 Certificate Output 5	FLASH Memory	TLS Client	Plaintext	Automated	Electronic	
SME Key Input 1	Peer encryptor	SDRAM	Encrypted	Automated	Electronic	KTS 1

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SME Key Output 1	SDRAM	Peer encryptor	Encrypted	Automated	Electronic	KTS 1
SME Key Input 2	Peer encryptor	SDRAM	Encrypted	Automated	Electronic	KTS 2
SME Key Output 2	SDRAM	Peer encryptor	Encrypted	Automated	Electronic	KTS 2
TIM KDK Input 1	CM7	FLASH Memory	Encrypted	Manual	Electronic	
TIM KDK Input 2	SSH CLI	FLASH Memory	Encrypted	Manual	Electronic	
TIM KDK Output	FLASH Memory	CM7	Encrypted	Manual	Electronic	
Authentication Password Input 1	CM7	FLASH Memory	Encrypted	Manual	Electronic	
Authentication Password Input 2	SSH CLI	FLASH Memory	Encrypted	Manual	Electronic	
Authentication Password Input 3	CLI	FLASH Memory	Plaintext	Manual	Direct	
SNMPv3 Diffie Hellman Public Key Input	CM7	SDRAM	Plaintext	Automated	Electronic	KAS SNMP
SNMPv3 Diffie Hellman Public Key Output	SDRAM	CM7	Plaintext	Automated	Electronic	KAS SNMP
SSH Public Key Input 1	CM7	FLASH Memory	Encrypted	Manual	Electronic	
SSH Public Key Input 2	SSH CLI	FLASH Memory	Encrypted	Manual	Electronic	
SSH Public Key Input 3	CLI	FLASH Memory	Plaintext	Manual	Electronic	
SSH Public Key Output	FLASH Memory	CM7	Encrypted	Manual	Electronic	
SSH Key Exchange Public Key Input	SSH Client/Server	SDRAM	Plaintext	Automated	Electronic	KAS SSH
SSH Key Exchange Public Key Output	SDRAM	SSH Client/Server	Plaintext	Automated	Electronic	KAS SSH
TLS Key Exchange Public Key Input	TLS Client/Server	SDRAM	Plaintext	Automated	Electronic	KAS TLS
TLS Key Exchange Public Key Output	SDRAM	TLS Client/Server	Plaintext	Automated	Electronic	KAS TLS

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The module's SSP zeroisation methods are detailed in the table below.

Zeroization Method	Description	Rationale	Operator Initiation
Tamper Event	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 SSPs is the same.	The tamper initiated zeroization process achieves the following: 1. Zeroization of the System Master Key (SMK) rendering CSPs stored in FLASH memory 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 SSPs 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 SSPs 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 11.2).	
Emergency Erase Button	The "Emergency" Erase feature is initiated when the concealed front panel Emergency Erase button is depressed	Causes the same response as Tamper Event above.	Operator Initiated
Erase Command	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.	Once initiated the module Zeroization sequence immediately carries out the following: * Sets each session (CI) to DISCARD, before zeroizing the DEKs * Zeroizes the SMK rendering CSPs stored in FLASH memory indecipherable. * Deletes CSPs stored in FLASH memory, module configuration and all certificate information. * Automatically REBOOTs the module destroying all SSPs residing in volatile system memory.	Operator Initiated
Power Cycle	Module Power Cycle	Sensitive data stored in a device's memory is securely erased by initiating a system power-off followed by a restart.	Operator Initiated

Table 18: SSP Zeroization Methods

9.4 SSPs

The module’s SSPs are detailed in the table below.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
System Master Key (SMK)	AES key used to encrypt CSPs stored in FLASH memory	256 bits - 256 bits	Symmetric Key - CSP	Generate Symmetric Key 1 (Direct generation from DRBG)		Symmetric Encryption/Decryption SMK
Triple-DES System Master Key	Used to decrypt CSPs stored in FLASH memory during upgrade from legacy software version.	192 bits - 168 bits	Symmetric Key - CSP			Symmetric Decryption SMK

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	They are re-encrypted using AES 256 SMK (see row above)					
SMK_Local	When KeySecure is configured, the local System Master Key (SMK_local) is generated from the internal DRBG and stored it in tamper protected memory.	256 bits - 256 bits	Symmetric Key component - CSP	Generate Symmetric Key 1 (Direct generation from DRBG)		
SMK_Mask	When KeySecure is configured, the module will obtain a System Master Key mask (SMK_mask) from the external KeySecure server.	256 bits - 256 bits	Symmetric Key component - PSP			
SMK_CSP	SMK_local and SMK_mask are combined to create SMK_CSP which is used to encrypt and decrypt the CSPs stored in FLASH memory.	256 bits - 256 bits	Symmetric Key - CSP	Generate Symmetric Key 2 (Symmetric Keys Produced by Combining (Multiple) Keys and Other Data)		Symmetric Encryption/Decryption SMK
Activation RSA Private Key	Used to unwrap/decapsulate user credentials sent from CM7 to module	2048 bits - 112 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 1 (RSA)		KTS 1
Activation RSA Public Key	Used to wrap/encapsulate user credentials sent from CM7 to module	2048 bits - 112 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 1 (RSA)		KTS 1
RSA Private Keys	Used for authentication and key wrapping between modules	2048 bits - 112 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 1 (RSA)		Authentication SME 1 Authentication TLS 1
RSA Public Keys	Used for authentication and key wrapping between modules	2048 bits - 112 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 1 (RSA)		Authentication SME 1 Authentication TLS 1
ECDSA Private Keys	Used for authentication between modules	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 2 (EC)		Authentication SME 2 Authentication TLS 2
ECDSA Public Keys	Used for authentication between modules	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 2 (EC)		Authentication SME 2 Authentication TLS 2
SME ECDH Private Keys	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.	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 2 (EC)		KAS SME

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SME ECDH Public Keys	Established during the SME key agreement process and destroyed once the process is complete. The ECDH Ephemeral Public Key is used to create the shared secret.	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 2 (EC)		KAS SME
SME ECDH Shared Secret	Established during the SP 800-56Arev3 compliant ECDHE key agreement	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Shared Secret - CSP		KAS SME	KAS SME
X509v3 Certificates	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.	-	X509v3 Certificate - PSP			Authentication SME 1 Authentication SME 2 Authentication TLS 1 Authentication TLS 2
Authentication Passwords	Up to 30 unique Crypto Officers (Administrators, Supervisors, Upgraders) or Users (Operators) may be defined, with associated passwords, within the module.	8-29 ASCII characters -	Password - CSP			
Authentication Password Hash		256 bits -	Secure Hash - CSP	Secure Hash		
Key Encrypting Keys (KEK)	For each RSA based session (CI) and EC Multipoint sessions, the AES KEK is derived from the SME KDK or SME GDK respectively, using an 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.	256 bits - 256 bits	Symmetric Key - CSP	KDF SME		KTS 2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Encrypting Keys (DEK)	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 with the 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	123 bits, 256 bits - 123 bits, 256 bits	Symmetric Key - CSP	KDF TIM Generate Symmetric Key 1 (Direct generation from DRBG)	KAS SME	Symmetric Encryption/Decryption Data Plane 1 Symmetric Encryption/Decryption Data Plane 2 Symmetric Encryption/Decryption Data Plane 3 Symmetric Encryption/Decryption Data Plane 4 Symmetric Encryption/Decryption Data Plane 5 Symmetric Encryption/Decryption Data Plane 6
TIM KDK	The KDK is used to derive the DEKs using a SP 800-108 compliant KDF.	256 bits -	Key Derivation Key - CSP	Generate Symmetric Key 1 (Direct generation from DRBG)		KDF TIM
Group Establishment Keys (GEK)	The GEK is used to wrap the group SME KDKs and initial DEKs using AES-256 CFB authenticated with HMAC-SHA-256.	256 bits - 256 bits	Symmetric Key - CSP	KDF SME		KTS 2
SME HMAC keys	The SME HMAC keys are used to protect the integrity of the AES key wrapped messages between encryptors.	256 bits - 256 bits	Integrity - CSP	KDF SME		KTS 2
SME KDK	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.	256 bits -	Key Derivation Key - CSP	Generate Symmetric Key 1 (Direct generation from DRBG)		KDF SME
Group Derivation Keys (GDK)	When a subordinate joins an ECDSA/ECDH VLAN or multicast group session the key master	256 bits -	Key Derivation Key - CSP		KAS SME	KDF SME

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	from the group and the subordinate 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 Diffie Hellman Private Keys	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	2048 bits - 112 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 3 (DH Key Generation during Key Agreement)		KAS SNMP
SNMPv3 Diffie Hellman Public Keys	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.	2048 bits - 112 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 3 (DH Key Generation during Key Agreement)		KAS SNMP
SNMPv3 Diffie Hellman Shared Secret	The shared secret is created during the SNMPv3 DH key agreement process	2048 bits - 112 bits	Shared Secret - CSP		KAS SNMP	KDF SNMP
SNMPv3 Privacy Keys	For each SNMPv3 remote management session, the module uses an AES privacy key established during DH key agreement process to secure the control / flow path in the secure connection.	128 bits, 256 bits - 128 bits, 256 bits	Symmetric Key - CSP	KDF SNMP		Symmetric Encryption/Decryption SNMPv3
SNMPv3 Integrity Keys	The SNMPv3 Integrity keys are used to protect the integrity of the data transmitted across the secure SNMP connection	160 bits, 512 bits - 160 bits, 512 bits	Symmetric Key - CSP	KDF SNMP		Message Authentication SNMP
DRBG Seed	Used as input for SP 800-90Ar1 Hash_DRBG	440 bits -	Input to DRBG - CSP	DRBG Request		DRBG Request
DRBG Entropy Input and Nonce	Used as input for SP 800-90Ar1 Hash_DRBG	384 bits -	Input to DRBG - CSP	Entropy Source		DRBG Request
DRBG V and C internal state parameters	The V and C parameters store the internal state of the SP 800-90rev1 DRBG	440 bits -	DRBG State Variables - CSP	DRBG Request		DRBG Request
SSH Private Keys	ECDSA key used to authenticate the module with the remote client/server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 2 (EC)		Authentication SSH
SSH Public Keys	ECDSA key used to authenticate the module with the remote client/server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 2 (EC)		Authentication SSH

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH Key Exchange Private Keys	ECDH key created for each SSH session to enable agreement of the SSH shared secret between the module and the remote client/server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 2 (EC)		KAS SSH
SSH Key Exchange Public Keys	ECDH key created for each SSH session to enable agreement of the SSH shared secret between the module and the remote client/server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 2 (EC)		KAS SSH
SSH Shared Secret	Used to derive the SSH Privacy and Integrity Keys	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Shared Secret - CSP		KAS SSH	KDF SSH
SSH Privacy Keys	Generated during the SSH I key agreement process and used for encryption of the data transmitted across the secure SSH connection	128 bits, 256 bits - 128 bits, 256 bits	Symmetric Key - CSP	KDF SSH		Symmetric Encryption/Decryption SSH
SSH Integrity Keys	The SSH Integrity keys are used to protect the integrity of the data transmitted across the secure SSH connection	256 bits, 512 bits - 256 bits, 512 bits	Integrity Key - CSP	KDF SSH		Message Authentication SSH
TLS Private Keys	Used to authenticate the module with the remote client/server	P-256, P-384, P-521, 2048 bits - 128 bits, 192 bits, 256 bits, 112 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 1 (RSA) Generate Asymmetric Keys 2 (EC)		Authentication TLS 1 Authentication TLS 2
TLS Public Keys	Used to authenticate the module with the remote client/server	P-256, P-384, P-521, 2048 bits - 128 bits, 192 bits, 256 bits, 112 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 1 (RSA) Generate Asymmetric Keys 2 (EC)		Authentication TLS 1 Authentication TLS 2
TLS Key Exchange Private Keys	The ECDH key is created for each TLS session to enable agreement of the TLS shared secret between the module and the remote server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 2 (EC)		KAS TLS
TLS Key Exchange Public Keys	The ECDH key is created for each TLS session to enable agreement of the TLS shared secret between the module and the remote server	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 2 (EC)		KAS TLS
TLS Premaster Secrets	The TLS Premaster Secret is used to generate the TLS Master Secret	384 bits -	Shared secret - CSP		KAS TLS	KDF TLS
TLS Master Secrets	The TLS Master Secret is used to derive TLS Privacy and Integrity keys	384 bits -	Key Derivation Key - CSP	KDF TLS		KDF TLS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Privacy Keys	Generated during the TLS key agreement process and used for encryption of the data transmitted across the secure TLS connection	128 bits, 256 bits - 128 bits, 256 bits	Symmetric Key - CSP	KDF TLS		Symmetric Encryption/Decryption TLS
TLS Integrity Keys	The TLS Integrity keys are used to protect the integrity of the data transmitted across the secure TLS connection	256 bits, 384 bits - 256 bits, 384 bits	Integrity Key - CSP	KDF TLS		Message Authentication TLS
Keyvault Private Keys	Used for Keyvault operations	P-256, P-384, P-521, 2048 bits - 128 bits, 192 bits, 256 bits, 112 bits	Asymmetric Key - CSP	Generate Asymmetric Keys 1 (RSA) Generate Asymmetric Keys 2 (EC)		KTS 1 Sign X.509 Certificate
Keyvault Public Keys	Used for Keyvault operations	P-256, P-384, P-521, 2048 bits - 128 bits, 192 bits, 256 bits, 112 bits	Asymmetric Key - PSP	Generate Asymmetric Keys 1 (RSA) Generate Asymmetric Keys 2 (EC)		KTS 1
Firmware Upgrade RSA Public Key	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	2048 bits - 112 bits	Asymmetric Key - PSP	Factory Installed		Firmware Load Test

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
System Master Key (SMK)		BBRAM:Plaintext		Tamper Event Emergency Erase Button Erase Command	
Triple-DES System Master Key		BBRAM:Plaintext		Tamper Event Emergency Erase Button Erase Command	
SMK_Local		BBRAM:Plaintext		Tamper Event Emergency Erase Button Erase Command	SMK_Mask:Combined with
SMK_Mask	Keysecure Input	SDRAM:Plaintext	Zeroised after use	Power Cycle	SMK_Local:Combined with
SMK_CSP		SDRAM:Plaintext	Zeroised after use	Power Cycle	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Activation RSA Private Key		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	Activation RSA Public Key:Paired With
Activation RSA Public Key	Activation Public Key Output	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	Activation RSA Private Key:Paired With
RSA Private Keys		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	RSA Public Keys:Paired With
RSA Public Keys	SME Public Key Input 1 SME Public Key Output 1	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	RSA Private Keys:Paired With
ECDSA Private Keys		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	ECDSA Public Keys:Paired With
ECDSA Public Keys	SME Public Key Input 1 SME Public Key Output 1	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	ECDSA Private Keys:Paired With
SME ECDH Private Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SME ECDH Public Keys:Paired With
SME ECDH Public Keys	SME Public Key Input 2 SME Public Key Output 2	SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SME ECDH Private Keys:Paired With
SME ECDH Shared Secret		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SME ECDH Private Keys:Agreed using SME ECDH Public Keys:Agreed using

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
X509v3 Certificates	X509v3 Certificate Input 1 X509v3 Certificate Input 2 X509v3 Certificate Input 3 X509v3 Certificate Input 4 X509v3 Certificate Input 5 X509v3 Certificate Output 1 X509v3 Certificate Output 2 X509v3 Certificate Output 3 X509v3 Certificate Output 4 X509v3 Certificate Output 5	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	RSA Public Keys:Associated with ECDSA Public Keys:Associated with TLS Public Keys:Associated with Keyvault Public Keys:Associated with
Authentication Passwords	Authentication Password Input 1 Authentication Password Input 2 Authentication Password Input 3	FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	
Authentication Password Hash		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	
Key Encrypting Keys (KEK)		SDRAM:Plaintext	The KEK persists for the life of the session	Tamper Event Emergency Erase Button Power Cycle	SME KDK:Derived From Group Derivation Keys (GDK):Derived From
Data Encrypting Keys (DEK)	SME Key Input 1 SME Key Output 1 SME Key Input 2 SME Key Output 2	SDRAM:Plaintext	The DEKs are updated when the key change interval expirers	Tamper Event Emergency Erase Button Power Cycle	
TIM KDK	TIM KDK Input 1 TIM KDK Input 2 TIM KDK Output	FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	
Group Establishment Keys (GEK)		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	Group Derivation Keys (GDK):Derived From
SME HMAC keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	Group Derivation Keys (GDK):Derived From SME KDK:Derived From
SME KDK	SME Key Input 1 SME Key Output 1 SME Key Input 2 SME Key Output 2	SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Group Derivation Keys (GDK)		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	
SNMPv3 Diffie Hellman Private Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SNMPv3 Diffie Hellman Public Keys:Paired With
SNMPv3 Diffie Hellman Public Keys	SNMPv3 Diffie Hellman Public Key Input SNMPv3 Diffie Hellman Public Key Output	SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SNMPv3 Diffie Hellman Private Keys:Paired With
SNMPv3 Diffie Hellman Shared Secret		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SNMPv3 Diffie Hellman Private Keys:Agreed Using SNMPv3 Diffie Hellman Public Keys:Agreed Using
SNMPv3 Privacy Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SNMPv3 Diffie Hellman Shared Secret:Derived From
SNMPv3 Integrity Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SNMPv3 Diffie Hellman Shared Secret:Derived From
DRBG Seed		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	DRBG Entropy Input and Nonce:Created From
DRBG Entropy Input and Nonce		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	
DRBG V and C internal state parameters		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	DRBG Seed:Associated with
SSH Private Keys		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	SSH Public Keys:Paired With
SSH Public Keys	SSH Public Key Input 1 SSH Public Key Input 2 SSH Public Key Input 3 SSH Public Key Output	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	SSH Private Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH Key Exchange Private Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SSH Key Exchange Public Keys:Paired With
SSH Key Exchange Public Keys	SSH Key Exchange Public Key Input SSH Key Exchange Public Key Output	SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SSH Key Exchange Private Keys:Paired With
SSH Shared Secret		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SSH Key Exchange Private Keys:Agreed Using SSH Key Exchange Public Keys:Agreed Using
SSH Privacy Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SSH Shared Secret:Derived From
SSH Integrity Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	SSH Shared Secret:Derived From
TLS Private Keys		FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	TLS Public Keys:Paired With
TLS Public Keys	X509v3 Certificate Input 1 X509v3 Certificate Input 2 X509v3 Certificate Input 3 X509v3 Certificate Output 1 X509v3 Certificate Output 2 X509v3 Certificate Output 3	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	TLS Private Keys:Paired With
TLS Key Exchange Private Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Key Exchange Public Keys:Paired With
TLS Key Exchange Public Keys	TLS Key Exchange Public Key Input TLS Key Exchange Public Key Output	SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Key Exchange Private Keys:Paired With
TLS Premaster Secrets		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Key Exchange Private Keys:Agreed Using TLS Key Exchange Public Keys:Agreed Using
TLS Master Secrets		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Premaster Secrets:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS Privacy Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Master Secrets:Derived From
TLS Integrity Keys		SDRAM:Plaintext	Zeroised after use	Tamper Event Emergency Erase Button Power Cycle	TLS Master Secrets:Derived From
Keyvault Private Keys	Keyvault Backup Keyvault Restore	FLASH Memory:Encrypted		Tamper Event Emergency Erase Button Erase Command	Keyvault Public Keys:Paired With
Keyvault Public Keys	Keyvault Backup Keyvault Restore	FLASH Memory:Plaintext		Tamper Event Emergency Erase Button Erase Command	Keyvault Private Keys:Paired With
Firmware Upgrade RSA Public Key		FLASH Memory:Plaintext		N/A	

Table 20: SSP Table 2

9.5 Transitions

Please see the latest revision of SP 800-131 and CMVP Programmatic Transitions page for transitions that may affect this module.

9.6 Additional Information

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 the CSPs stored in FLASH memory it will retrieve SMK_local and SMK_mask and combine them to create SMK_CSP which is used to perform the operation.

This feature allows centralised management of SSPs within a network of encryptors. Deleting SMK_mask in the KeySecure server will destroy the SSPs 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.

10 Self-Tests

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 Encryptors ensures that all data output, via the data output interface and management interfaces, 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 SHA2-256 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 LCD will display a message stating that the self-tests passed and the module will allow access via the CLI and remote management tools. The data-plane ports will be enabled and normal operation will commence.

The module's pre-operational self-tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A3451)		Integrity Test	SW/FW Integrity	Audit Log	A 32-byte SHA2-256 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 SHA2-256 algorithm is tested using a KAT prior to the Software/ Firmware integrity test running.
Bypass Policy			Bypass	Audit Log	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).
RTC/ Tamper			Critical Function	Audit Log	Tamper memory is examined for evidence of a Tamper Condition.

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

A set of conditional self-tests run when required.

The conditional cryptographic algorithm known answer tests are run during the power up (pre-operational) sequence.

The module's conditional self-tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A3451)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CFB128 (A3451)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3451)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
ECDSA SigGen (FIPS186-4) (A3451)	P-256, P-384, P-521	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-4) (A3451)	P-256, P-384, P-521	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
ECDSA KeyGen (FIPS186-4) (A3451)	P-256, P-384, P-521	PCT	PCT	Audit Log	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	Key Pair Generation
Hash DRBG (A3451)	256-bit	KAT	CAST	Audit Log	SP 800-90 A Section 11.3 (Instantiate, Reseed, Generate and Un-instantiate)	Power Up
HMAC-SHA-1 (A3451)	160-bit	KAT	CAST	Audit Log	MAC	Power Up
HMAC-SHA2-256 (A3451)	256-bit	KAT	CAST	Audit Log	MAC	Power Up
HMAC-SHA2-384 (A3451)	384-bit	KAT	CAST	Audit Log	MAC	Power Up
HMAC-SHA2-512 (A3451)	512-bit	KAT	CAST	Audit Log	MAC	Power Up
KAS-ECC Sp800-56Ar3 (A3451)	P-256, P-384, P-521	KAT	CAST	Audit Log	ECDH (Cofactor) Ephemeral Unified Model SP 800-56Arev3	Power Up
ECDH PCT	P-256, P-384, P-521	PCT	PCT	Audit Log	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.	Key Pair Generation
KAS-FFC Sp800-56Ar3 (A3451)	2048-bit	KAT	CAST	Audit Log	DH dhEphem 2048 MODP group SP 800-56Arev3	Power Up
Safe Primes Key Generation (A3451)	2048-bit	PCT	PCT	Audit Log	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.	Key Pair Generation
KDF SNMP (A3451)	160-bit, 256-bit	KAT	CAST	Audit Log	Key Derivation	Power Up
KDF SP800-108 (A3451)	256-bit	KAT	CAST	Audit Log	Key Derivation	Power Up
KDF SSH (A3451)	256-bit, 512-bit	KAT	CAST	Audit Log	Key Derivation	Power Up
TLS v1.2 KDF RFC7627 (A3451)	256-bit, 384-bit	KAT	CAST	Audit Log	Key Derivation	Power Up
KTS-IFC (A3451)	2048-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A3451)	2048-bit	KAT	CAST	Audit Log	Sign/ Verify	Power Up
RSA SigVer (FIPS186-4) (A3451)	2048-bit	KAT	CAST	Audit Log	Sign/ Verify	Power Up
RSA KeyGen (FIPS186-4) (A3451)	2048-bit	PCT	PCT	Audit Log	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	Key Pair Generation
SHA-1 (A3451)	160-bit	KAT	CAST	Audit Log	Secure Hash	Power Up
SHA2-256 (A3451)	256-bit	KAT	CAST	Audit Log	Secure Hash	Power Up
SHA2-384 (A3451)	384-bit	KAT	CAST	Audit Log	Secure Hash	Power Up
SHA2-512 (A3451)	512-bit	KAT	CAST	Audit Log	Secure Hash	Power Up
TDES-CFB8 (A3451)	192-bit	KAT	CAST	Audit Log	Decrypt	Power Up
AES-CFB128 (A3435)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3435)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3435)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3436)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3436)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CFB128 (A3437)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3437)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3437)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3438)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3438)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CFB128 (A3439)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A3439)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3439)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3440)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3440)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3459)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3459)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3458)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3458)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CFB128 (A3549)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3549)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3549)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3443)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3443)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3441)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3441)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3442)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3442)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CFB128 (A3445)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3445)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3445)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3460)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3460)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A3448)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3448)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3444)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3444)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3492)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3446)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3446)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-CTR (A3447)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
AES-GCM (A3447)	128-bit, 256-bit	KAT	CAST	Audit Log	Separate Encrypt and Decrypt	Power Up
SHA2-256 Bypass Parameter Integrity	256-bit		Bypass	Audit Log	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 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.	Process Initialisation
Firmware Load Test	RSA SigVer	Signature Verification	SW/FW Load	Audit Log	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	Firmware Load
Battery			Critical Function	Audit Log	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	Continuous

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RTC / Tamper Memory			Critical Function	Audit Log	The Real Time Clock (RTC) oscillator is checked at start-up and the Tamper memory is examined continuously for evidence of a Tamper Condition.	Continuous
Repetition Count Test (RCT)		FD	CAST	Audit Log	SP 800-90B Section 4	Power Up, On Demand and Continuously
Adaptative Proportion Test (APT)		FD	CAST	Audit Log	SP 800-90B Section 4	Power Up, On Demand and Continuously

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

A subset of the pre-operational tests run periodically. The Bypass/Encrypt Policy test and 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 dependent.

The module's periodic self-tests are detailed in the table below.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A3451)	Integrity Test	SW/FW Integrity	24 Hours	Automatic
Bypass Policy		Bypass	24 Hours	Automatic
RTC/ Tamper		Critical Function	Continuous	Automatic

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3451)	KAT	CAST		
AES-CFB128 (A3451)	KAT	CAST		
AES-GCM (A3451)	KAT	CAST		
ECDSA SigGen (FIPS186-4) (A3451)	KAT	CAST		
ECDSA SigVer (FIPS186-4) (A3451)	KAT	CAST		
ECDSA KeyGen (FIPS186-4) (A3451)	PCT	PCT		
Hash DRBG (A3451)	KAT	CAST		
HMAC-SHA-1 (A3451)	KAT	CAST		
HMAC-SHA2-256 (A3451)	KAT	CAST		
HMAC-SHA2-384 (A3451)	KAT	CAST		
HMAC-SHA2-512 (A3451)	KAT	CAST		

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC Sp800-56Ar3 (A3451)	KAT	CAST		
ECDH PCT	PCT	PCT		
KAS-FFC Sp800-56Ar3 (A3451)	KAT	CAST		
Safe Primes Key Generation (A3451)	PCT	PCT		
KDF SNMP (A3451)	KAT	CAST		
KDF SP800-108 (A3451)	KAT	CAST		
KDF SSH (A3451)	KAT	CAST		
TLS v1.2 KDF RFC7627 (A3451)	KAT	CAST		
KTS-IFC (A3451)	KAT	CAST		
RSA SigGen (FIPS186-4) (A3451)	KAT	CAST		
RSA SigVer (FIPS186-4) (A3451)	KAT	CAST		
RSA KeyGen (FIPS186-4) (A3451)	PCT	PCT		
SHA-1 (A3451)	KAT	CAST		
SHA2-256 (A3451)	KAT	CAST		
SHA2-384 (A3451)	KAT	CAST		
SHA2-512 (A3451)	KAT	CAST		
TDES-CFB8 (A3451)	KAT	CAST		
AES-CFB128 (A3435)	KAT	CAST		
AES-CTR (A3435)	KAT	CAST		
AES-GCM (A3435)	KAT	CAST		
AES-CTR (A3436)	KAT	CAST		
AES-GCM (A3436)	KAT	CAST		
AES-CFB128 (A3437)	KAT	CAST		
AES-CTR (A3437)	KAT	CAST		
AES-GCM (A3437)	KAT	CAST		
AES-CTR (A3438)	KAT	CAST		
AES-GCM (A3438)	KAT	CAST		
AES-CFB128 (A3439)	KAT	CAST		
AES-CTR (A3439)	KAT	CAST		
AES-GCM (A3439)	KAT	CAST		
AES-CTR (A3440)	KAT	CAST		

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3440)	KAT	CAST		
AES-CTR (A3459)	KAT	CAST		
AES-GCM (A3459)	KAT	CAST		
AES-CTR (A3458)	KAT	CAST		
AES-GCM (A3458)	KAT	CAST		
AES-CFB128 (A3549)	KAT	CAST		
AES-CTR (A3549)	KAT	CAST		
AES-GCM (A3549)	KAT	CAST		
AES-CTR (A3443)	KAT	CAST		
AES-GCM (A3443)	KAT	CAST		
AES-CTR (A3441)	KAT	CAST		
AES-GCM (A3441)	KAT	CAST		
AES-CTR (A3442)	KAT	CAST		
AES-GCM (A3442)	KAT	CAST		
AES-CFB128 (A3445)	KAT	CAST		
AES-CTR (A3445)	KAT	CAST		
AES-GCM (A3445)	KAT	CAST		
AES-CTR (A3460)	KAT	CAST		
AES-GCM (A3460)	KAT	CAST		
AES-CTR (A3448)	KAT	CAST		
AES-GCM (A3448)	KAT	CAST		
AES-CTR (A3444)	KAT	CAST		
AES-GCM (A3444)	KAT	CAST		
AES-CTR (A3492)	KAT	CAST		
AES-CTR (A3446)	KAT	CAST		
AES-GCM (A3446)	KAT	CAST		
AES-CTR (A3447)	KAT	CAST		
AES-GCM (A3447)	KAT	CAST		
SHA2-256 Bypass Parameter Integrity		Bypass		
Firmware Load Test	Signature Verification	SW/FW Load		
Battery		Critical Function		
RTC / Tamper Memory		Critical Function		
Repetition Count Test (RCT)	FD	CAST		

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Adaptative Proportion Test (APT)	FD	CAST		

Table 24: Conditional Periodic Information

10.4 Error States

The module's self-test error states are described in the table below.

Name	Description	Conditions	Recovery Method	Indicator
Secure Halt	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.	Pre-Operational Software/ Firmware Integrity test failure Cryptographic KAT failure Pre-Operational RTC/ Tamper test failure RCT or APT Failure	Attempt to recover by power-cycle. If the Secure Halt condition persists the module cannot be recovered and must be returned to the factory.	LEDs flashing red (all models) and alarm message on LCD (CN6000 and CN9000 Series) Audit Log (if recoverable)
Configuration Erase	The module's policy configuration will be erased and reset to factory defaults. Global policy mode will be set to Discard preventing all data being transmitted over the Network data output interface.	Conditional Bypass Parameter Integrity test failure	Reconfigure and attempt to pass Network data	Audit Log
Global mode discard	If the Bypass Policy Test fails when the module is in the pre-operational or operational state, the global mode parameter is set to discard inhibiting all data being transmitted over the Network data output interface.	Bypass Policy test failure	Observe carefully and reconfigure unit, if error persists check "User Guide"	Audit Log
Error/Alarm	Error/Alarm logged. System state unchanged	PCT failure Conditional Software/Firmware Load test failure	Observe carefully and re-attempt, if error persists check "User Guide"	Audit Log

Table 25: Error States

10.5 Operator Initiation of 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.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

This section provides information for Crypto Officers to install, configure and operate the module in FIPS mode.

11.2 Administrator Guidance

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 a seal is broken, then the integrity of the encryptor cannot be assured and the supplier should be informed immediately.

Upon receipt of an 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.

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 Encryptors 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.

Administrator Guidance: Approved 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 Encryptors are 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. Refer to Figure 23 below.

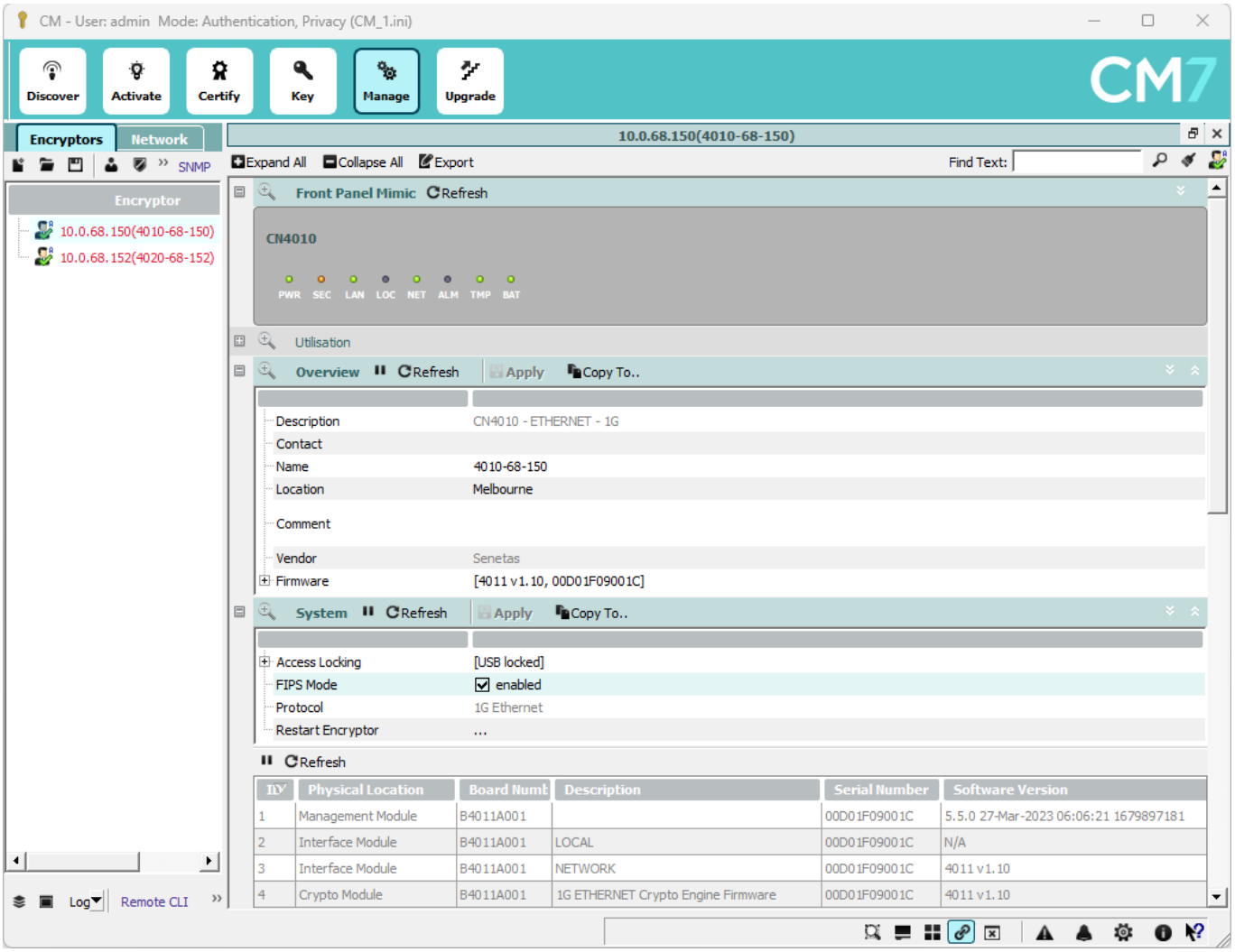

Figure 23 – "FIPS mode" selection

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

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 module automatically completes 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 Guides [26] 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 Encryptors 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 encryptor 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 an encryptor the administrator can create supervisor, upgrader and operator accounts.

   At this point the 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 application’s **Management-Access** tab. See Figure 23 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”.

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 Encryptors. Configuration of the security policy is network specific; refer to the User Guides [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.

11.3 Non-Administrator Guidance

Non-administrators (Operator privilege level) 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.

11.4 End of 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

12.1 Attack List

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.

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 provides 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.

12.2 Mitigation Effectiveness

By transmitting a constant stream of encrypted data, TRANSEC mode effectively prevents traffic flow analysis.

12.3 Guidance and Constraints

Please refer to the User Guides [26] for configuration instructions.

Please note that both encryptors must be operating at the same speed (bandwidth).