![Senetas logo - Security without compromise]

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

**CN6000 Series Encryptors**

**FIPS 140-2 Non-Proprietary Security Policy**
**Level 3 Validation**
**July 2022**

| | |
|---|---|
| **Module Name(s):** | **CN6000 Series Encryptors** |
| **Model Names:** | **CN6040 1G Ethernet Encryptor** |
| | **CN6100 10G Ethernet Encryptor** |
| **Module Version:** | **CN6000 Series:** |
| | **A6040B (AC), A6041B (DC), A6042B (AC/DC)** |
| | **A6100B (AC), A6101B (DC), A6102B (AC/DC)** |



CN6040 1G Ethernet Encryptor



CN6100 10G Ethernet Encryptor

www.senetas.com

# Table of Contents

Senetas Corp. Ltd.                        **Version 1.25**                        Page 2 of 60

CN6000 Series Non-Proprietary Security Policy

# 1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for the Senetas Corporation Ltd. CN6000 Series Encryptors comprising both the CN6040 and CN6100 (Firmware versions 5.2.0/5.2.1) cryptographic models. This Security Policy specifies the security rules under which the module operates to meet the FIPS 140-2 Level 3 requirements.

The CN6000 series of Ethernet Encryption devices are distributed worldwide under different brands as depicted in this Security Policy. The vendor distributes under their Senetas brand, Thales SA, the master worldwide distributor, distributes under the joint Thales/Senetas and SafeNet/Senetas brands.

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

This Security Policy, using the terminology contained in the FIPS 140-2 specification, describes how the CN6040 1G Ethernet Encryptor and the CN6100 10G Ethernet Encryptor models comply with the eleven sections of the standard. In this document, the CN6040 and CN6100 Encryptors are collectively referred to as the "CN6000 Series" and individually as "the module" or "the encryptor". The model name refers to all of the relevant module versions i.e. CN6040 refers to the module versions A6040B (AC), A6041B (DC), A6042B (AC/DC) (refer to Table 2 for a full listing).

This Security Policy and the associated CMVP certificate are for firmware versions 5.2.0/5.2.1 only – the loading of any other firmware version on the specified CN6000 Series Ethernet Encryption devices is out of scope of this FIPS 140-2 validation.

This Security Policy contains only non-proprietary information. Any other documentation associated with FIPS 140-2 conformance testing and validation is proprietary and confidential to Senetas Corporation Ltd. and is releasable only under appropriate non-disclosure agreements. For more information describing the CN6000 Series systems, visit http://www.senetas.com.

## 1.1    References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Senetas Corp. Ltd.                **Version 1.25**                Page 3 of 60

CN6000 Series Non-Proprietary Security Policy

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

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

## 1.2    Document History

| Authors | Date | Version | Comment |
|---|---|---|---|
| Senetas Corp. Ltd. | 28-Jul-2018 | 1.00 | Initial version for v5.0.1 firmware release |
| Senetas Corp. Ltd. | 24-Jun-2019 | 1.01 | Changes to address CSC comments |
| Senetas Corp. Ltd. | 17-Jan-2020 | 1.10 | Initial version for 5.1.0 firmware release |
| Senetas Corp. Ltd. | 06-Jan-2021 | 1.11 | Changes to address CMVP comments |
| Senetas Corp. Ltd. | 07-Apr-2021 | 1.12 | Changes to address CMVP comments |
| Senetas Corp. Ltd. | 20-Jul-2021 | 1.20 | Initial version for 5.2.0 firmware release |
| Senetas Corp. Ltd. | 29-Mar-2022 | 1.21 | Changes to address CMVP comments |
| Senetas Corp. Ltd. | 08-Apr-2022 | 1.22 | Changes to address CMVP comments |
| Senetas Corp. Ltd. | 19-Apr-2022 | 1.23 | Added FPGA firmware versions |
| Senetas Corp. Ltd. | 27-Apr-2022 | 1.24 | Updated KAS-FFC entries |
| Senetas Corp. Ltd. | 13-Jul-2022 | 1.25 | CMVP final v5.2.0/5.2.1 Security Policy |

## 1.3    Acronyms and Abbreviations

AAA            Authentication, Authorization and Accounting

AES            Advanced Encryption Standard

CA             Certification Authority

CBC            Cipher Block Chaining

CCCS           Canadian Centre for Cyber Security

CFB            Cipher Feedback

CM7            Senetas Encryptor Remote Management Application Software

CI             Connection Identifier (used interchangeably with Tunnel)

CLI            Command Line Interface

CMVP           Cryptographic Module Validation Program

CRNGT          Continuous Random Number Generator Test

CSE            Communications Security Establishment

CSP            Critical Security Parameter

CTR            Counter Mode

DEK            Data Encrypting Key(s)

DES            Data Encryption Standard

DH             Diffie-Hellman

DRBG           Deterministic Random Bit Generator

ECDH           Elliptic Curve Diffie-Hellman

Senetas Corp. Ltd.                    **Version 1.25**                    Page 4 of 60

CN6000 Series Non-Proprietary Security Policy

| | |
|---|---|
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| ENT (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 |
| GEK | Group Establishment Key |
| HMAC | Keyed-Hash Message Authentication Code |
| IP | Internet Protocol |
| ISID | Individual Service Identifier |
| 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 |
| 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 |
| NTU | Network Termination Unit |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| OAEP | Optimal Asymmetric Encryption Padding |
| OQS | Open Quantum Safe |
| PKCS | Public Key Cryptography Standards |
| PUB | Publication |
| QKD | Quantum Key Distribution |
| QRA | Quantum Resistant Algorithms |
| RAM | Random Access Memory |
| RFC | Request for Comment |
| ROM | Read Only Memory |
| RNG | Random Number Generator |
| RSA | Rivest Shamir and Adleman Public Key Algorithm |
| RTC | Real Time Clock |
| SAN | Storage Area Network |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 5 of 60

CN6000 Series Non-Proprietary Security Policy

| 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 |
| 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 |
| XFP | 10 Gigabit Small Form Factor Pluggable (transceiver) |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 6 of 60

CN6000 Series Non-Proprietary Security Policy

## 2. Product Description

CN6000 Series Encryptors are multiple-chip standalone cryptographic modules consisting of production-grade components contained, in accordance with FIPS 140-2 Level 3, in a physically protected enclosure. The module's outer casing defines the cryptographic boundary aside from the pluggable transceivers (XFP and SFP), dual redundant power supplies and replaceable fan tray module that lie outside the crypto boundary. All ventilation holes are protected by steel anti-probing barriers. The encryptor is completely enclosed in a metal case which is protected from tampering by internal tamper protection circuitry and external tamper evident seals. Any attempt to remove the cover automatically erases all sensitive information stored internally in the cryptographic module.

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

**Table 1    Module Compliance Table**

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 7 of 60

CN6000 Series Non-Proprietary Security Policy

## 2.1 Module Identification

CN6000 Series Encryptors, with firmware versions 5.2.0/5.2.1, provide data privacy and access control services for Ethernet networks. See model details summarized in Table 2.

Data privacy is provided by a FIPS approved AES algorithm. The complete list of approved module algorithms is included in the *Approved Security Function* table.

**Table 2 CN6000 Models: Hardware/Firmware Versions**

| Hardware Versions | Power | Interface / Protocol (Cryptographic Module) | Model Name | Firmware Versions |
|---|---|---|---|---|
| A6040B [O][1,2] A6040B [Y][1,2] A6040B [T][1,2] | AC | | | |
| A6041B [O][1,2] A6041B [Y][1,2] A6041B [T][1,2] | DC | 1G Ethernet | CN6040 | 5.2.0/5.2.1 |
| A6042B [O][1,2] A6042B [Y][1,2] A6042B [T][1,2] | AC/DC | | | |
| A6100B [O][1,3] A6100B [Y][1,3] A6100B [T][1,3] | AC | | | |
| A6101B [O][1,3] A6101B [Y][1,3] A6101B [T][1,3] | DC | 10G Ethernet 10G TIM | CN6100 | 5.2.0/5.2.1 |
| A6102B [O][1,3] A6102B [Y][1,3] A6102B [T][1,3] | AC/DC | | | |

**Table Notes:**

Note 1: Model variants distinguished by [O], [Y] and [T] are identical except for logos on the front fascia:
[O] Denotes Senetas Corp. Ltd. sole branded version
[Y] Denotes Senetas Corp. Ltd. & SafeNet co-branded version
[T] Denotes Senetas Corp. Ltd. & Thales SA co-branded version

Note 2: These models support pluggable SFP transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Note 3: These models support pluggable XFP transceivers, dual power supplies and removable fan tray which are considered to be outside the cryptographic boundary.

Senetas Corp. Ltd.          **Version 1.25**          Page 8 of 60

CN6000 Series Non-Proprietary Security Policy

**Figure 1 - Thales co-branding**



**Figure 2 – SafeNet co-branding**



**Figure 3 – Senetas sole-branding**

## 2.2 Operational Overview

### 2.2.1 General

CN6000 Series Encryptors operate in point-to-point and point-to-multipoint network topologies and at data rates ranging from 10Mb/s to 10Gb/s.

Encryptors are typically installed between an operator's private network equipment and public network connection and are used to secure data travelling over either fibre optic or CAT5/6 cables.

Securing a data link that connects two remote office sites is a common installation application.
*Figure 4* provides an operational overview of two CN6040 encryptors positioned in the network.
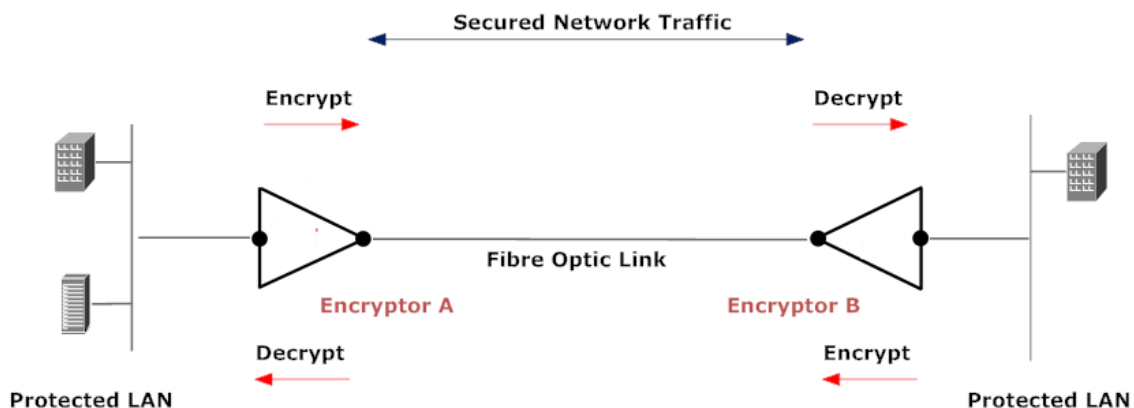


**Figure 4 – CN6040 Operational Overview**

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

CN6000 Series Non-Proprietary Security Policy

CN6000 Series Encryptors support CI Modes of 'Secure', 'Discard' and 'Bypass'. These CI Modes can be applied to all data carried on a connection or to a selected subset or grouping which can be user configured in accordance the specific protocol being carried on the network connection. A typical example in the case of an Ethernet network would be to make policy decisions based upon an Ethernet packet's VLAN ID.

The default CI Mode negotiated between a pair of connected encryptors is `Discard`. In this mode user data is not transmitted to the public network.

In order to enter `Secure` mode and pass information securely, each encryptor must be `Certified` by the same trusted body and exchange the key encrypting key (KEK) and initial data encryption key (DEK), using the RSA-OAEP-256 key transport process in accordance with NIST SP800-56B Rev2 Section 9. Alternatively, ECDSA/ECDH utilises ephemeral key agreement for the purpose of establishing DEKs in accordance with NIST SP800-56A Rev3. 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.

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 or the CLI. The KDK is used to derive the DEKs using a KDF that conforms to NIST SP 800-108.

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

Figure 5. illustrates the conceptual data flow through a CN6000 Series Encryptor.

1. A data packet arrives at the encryptor's interface ports. When operating in Line mode data packets are processed according to a single CI policy, otherwise,

2. The encryptor looks up the appropriate packet header field, e.g. MAC address, VLAN ID or ISID 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.
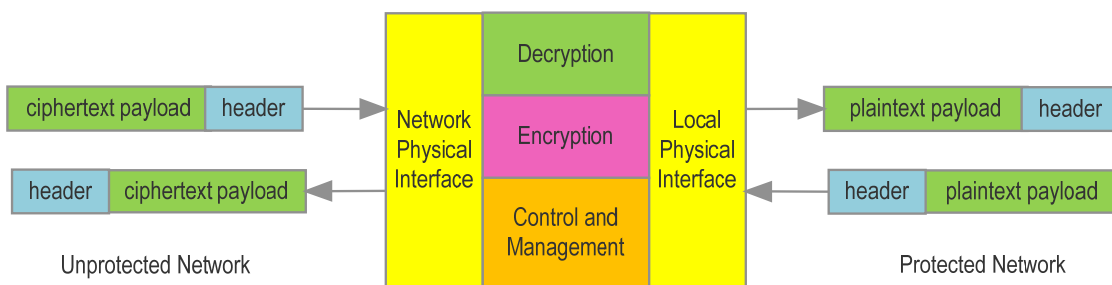


**Figure 5 - Data Flow through the Encryptor**

---

[1] TIM is not available on the CN6040.

Senetas Corp. Ltd.          **Version 1.25**                    Page 10 of 60

CN6000 Series Non-Proprietary Security Policy

### 2.2.2 Encryptor deployment

Figure 6 illustrates a point-to-point (or link) configuration in which each module connects with a single far end module and encrypts the entire bit stream. If a location maintains secure connections with multiple remote facilities, it will need a separate pair of encryptor's for each physical connection (link).
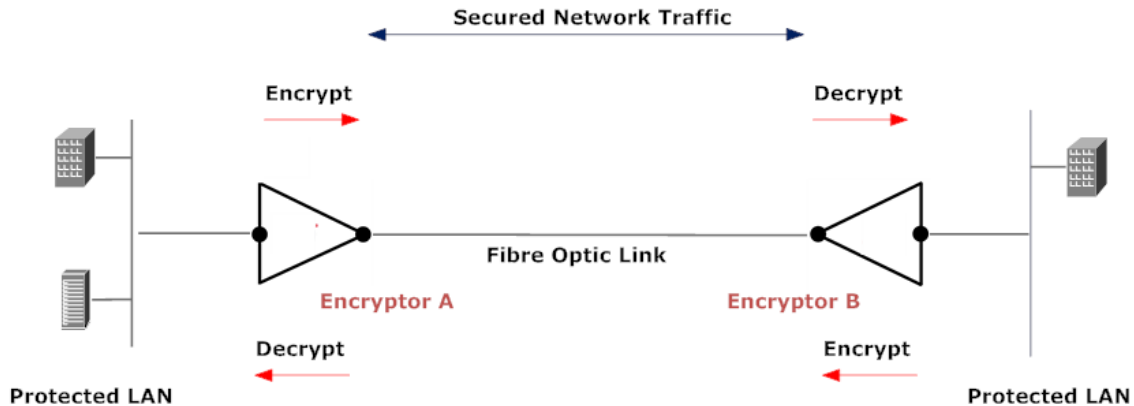


**Figure 6 - Link (point to point) Configuration**

Figure 7 illustrates a meshed network configuration.. Each CN6000 Series Encryptor is able to maintain simultaneous secured connections with many far end encryptors.
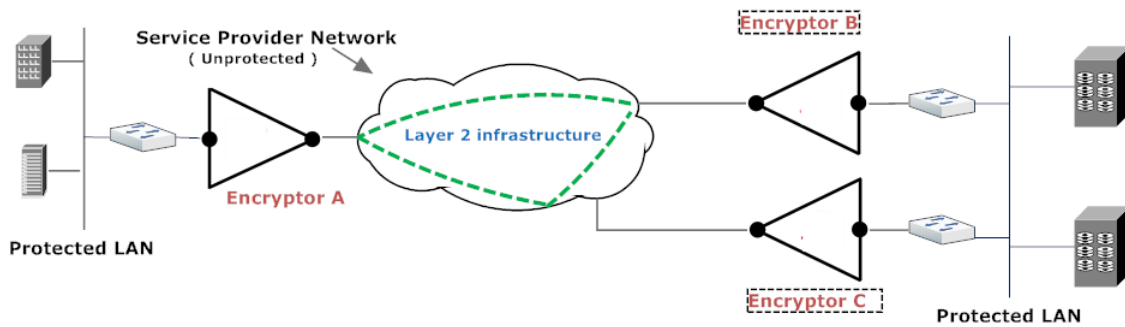


**Figure 7 - Meshed (multipoint) Configuration**

### 2.2.3 Encryptor management

Encryptors can be centrally controlled or managed across local and remote stations using the CM7 or SMC remote management application. The remote management applications reside outside the cryptographic boundary and are not in the scope of the FIPS validation. Encryptors support both *in-band* and *out-of-band* SNMPv3 management. *In-band* management interleaves management messages with user data on the encryptor's network interface port whilst *out-of-band* management uses the dedicated front panel Ethernet port. A Command Line Interface (CLI) is also available via the console RS-232 port. Alternatively the CLI can be accessed remotely via SSH (when configured). When configuring remote CLI access the authentication algorithm is restricted to ECDSA. The ECDSA keys are restricted to NIST P-256, P-384 and P-521 curves. Remote CLI access is disabled by default.

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

### 2.2.4 Ethernet implementation

**Basic operation**

Senetas Corp. Ltd.                    **Version 1.25**                    Page 11 of 60

CN6000 Series Non-Proprietary Security Policy

The Ethernet encryptor provides layer 2 security services by encrypting the contents of data frames across Ethernet networks. The encryptor connects between a local (protected) network and a remote (protected) network across the public (unprotected) network. An encryptor is paired with one or more remote Ethernet encryptors to provide secure data transfer over encrypted connections as shown in Figure 8 below.
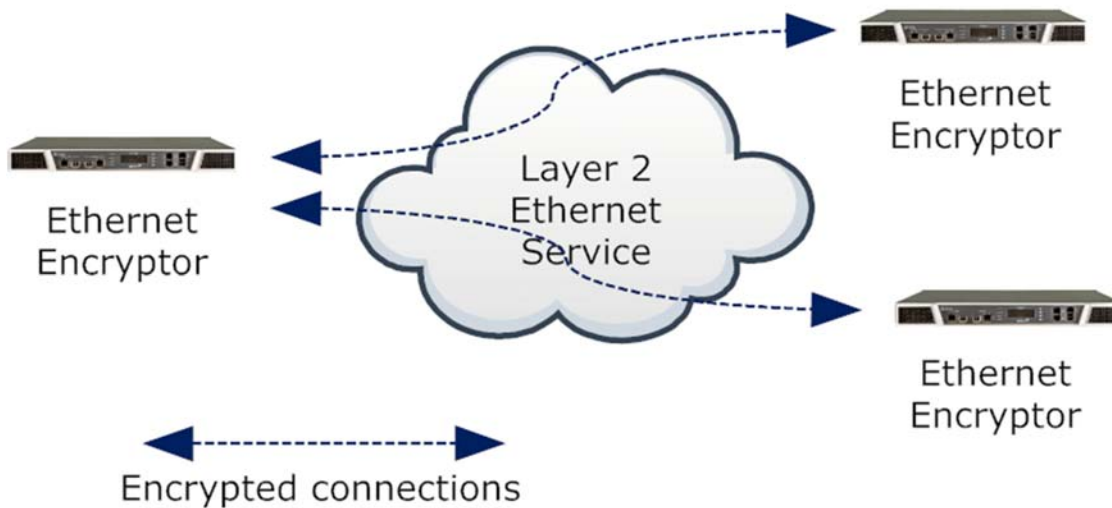


**Figure 8 – Layer 2 Ethernet connections**

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

CN6000 Series tunnels are encrypted using CAVP validated AES algorithms. The CN6040 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 10G Ethernet encryptors support AES encryption with a key size of 128 or 256 bits in counter (CTR) and Galois Counter (GCM) modes.

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

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

### 2.2.4.1 Unicast operation

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

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

## 2.2.4.2 Multipoint VLAN operation

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

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

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

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

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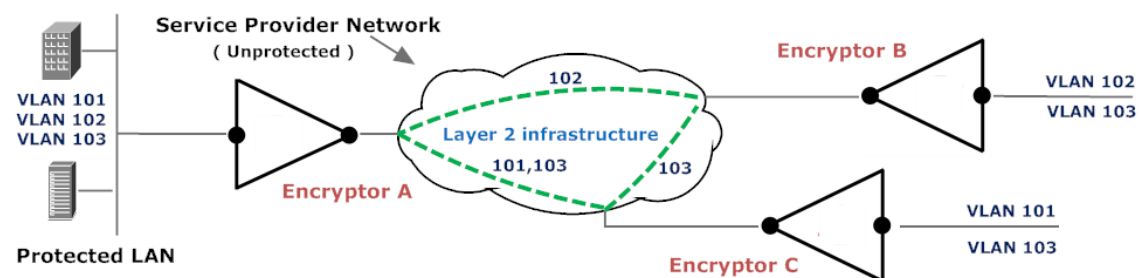


**Figure 9 – Multipoint VLAN connections**

## 2.2.4.3 Transport Independent Mode (TIM) operation

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

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

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

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

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

**TIM key updates**

In Transport Independent Mode keys are periodically updated using either a time based mechanism or a frame counter based mechanism.
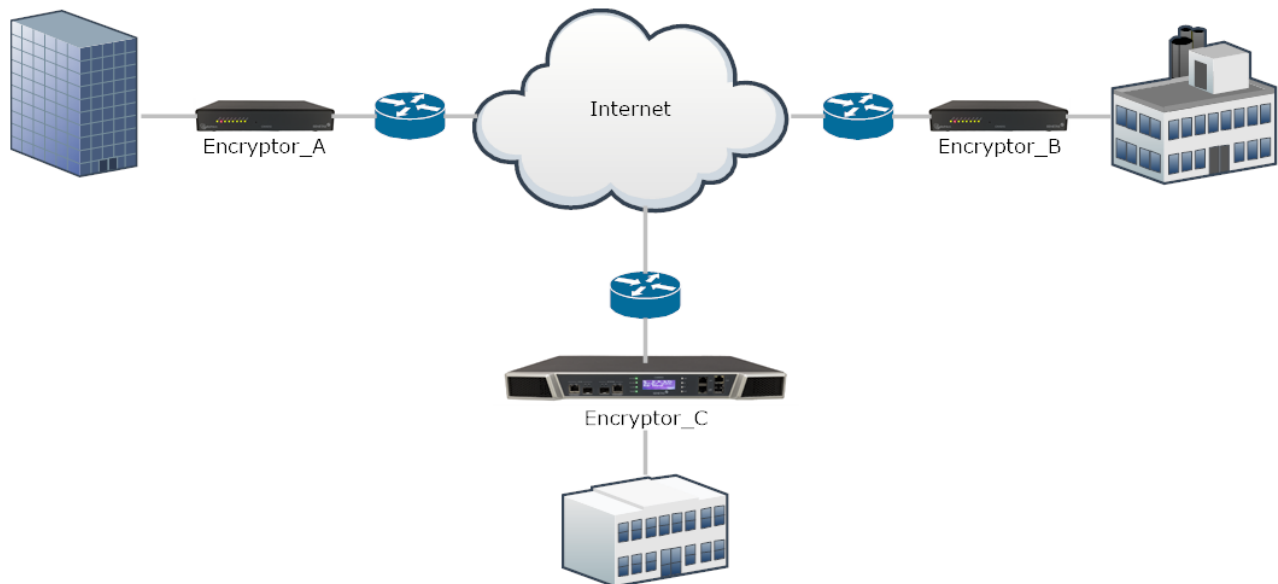
**Figure 10 – Transport Independent Mode connections**

### 2.2.5    Hybrid Key Establishment

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

#### 2.2.5.1 Quantum Resistant Algorithms (QRA)

The CN Series of encryptors support the use of candidate Quantum Resistant Algorithms as available from the Open Quantum Safe initiative. The user can select from a full list consisting of the RSA/ECDSA algorithms and the new OQS signing algorithms. The RSA/ECDH algorithms are used in parallel with the candidate Quantum Resistant Algorithms and the established keys are combined using an SP 800-56C compliant KDF in line with NIST guidance for post-quantum hybrid key establishment.

#### 2.2.5.2 Quantum Key Distribution (QKD)

The CN Series of 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 RSA/ECDH algorithms are combined with the QKD derived keys using an SP 800-56C compliant KDF.

### 2.2.6    TRANSEC operation

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

When operating in TRANSEC mode 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.

Senetas Corp. Ltd.                    **Version 1.25**                    Page 14 of 60

CN6000 Series Non-Proprietary Security Policy
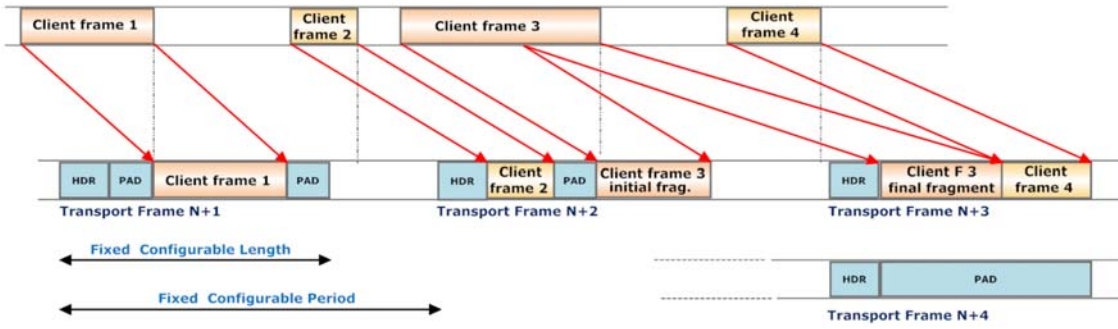
**Figure 11 – TRANSEC constant rate transport frame assembly**

CN6000 Series Non-Proprietary Security Policy

# 3. Module Ports and Interfaces

## 3.1 CN6000 Series Ports

The CN6000 Series data and management ports are located on the encryptor's front panel.

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

In the case of the CN6040 operating in Ethernet encryption mode, the operator can select either the RJ45 electrical or SFP optical physical interface to connect to the network.

The encryptor user access management ports, LCD display and Keypad are located on the front of the module.

The CN6040 and CN6100 models are depicted below.
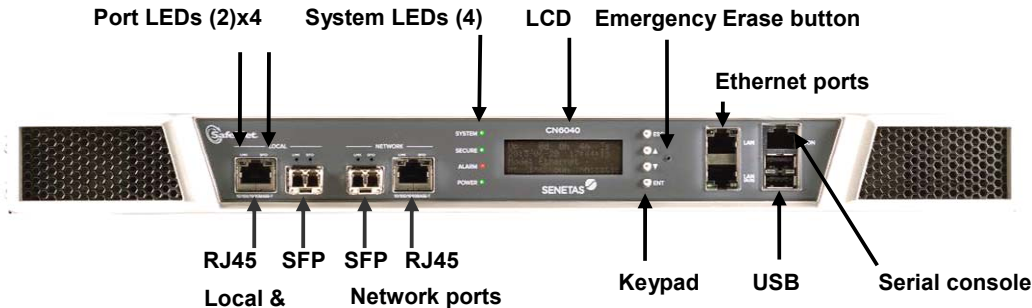


**Figure 12 - Front View of the CN6040 Encryptor**
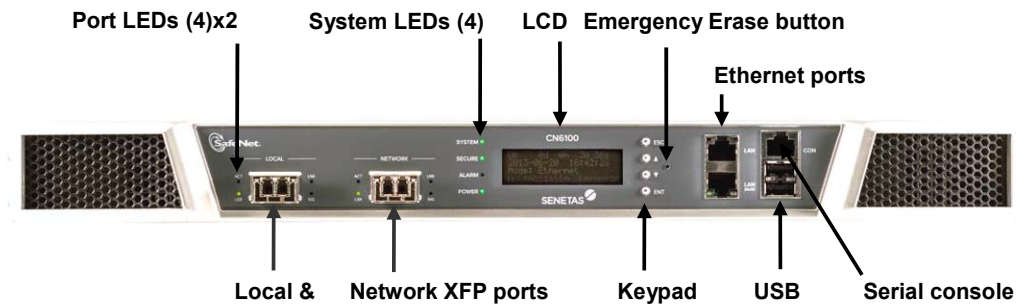


**Figure**

**13 - Front View of the CN6100 Encryptor**

Senetas Corp. Ltd.          **Version 1.25**          Page 16 of 60

CN6000 Series Non-Proprietary Security Policy

CN6000 Series Encryptors support dual redundant power supplies which are available in two variants, an AC version for typical installs and a DC version for telecoms applications. Any power supply combination i.e. AC/AC, AC/DC or DC/DC is supported.  Details of each can be seen in Figure 14.
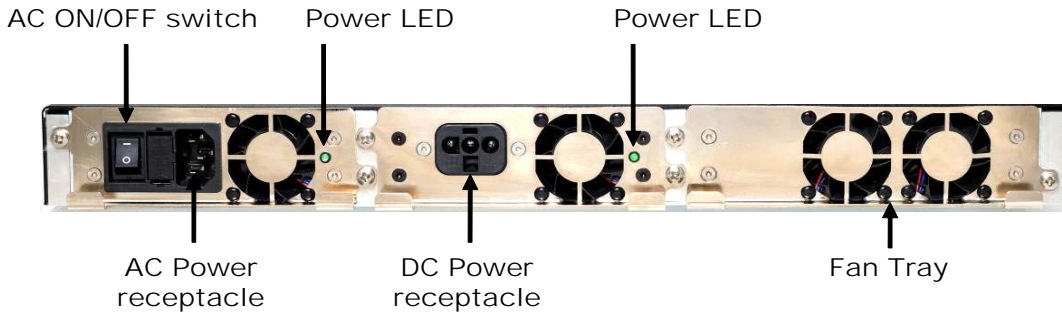


**Figure 14 - Rear View: CN6000 Series Encryptor pictured with AC & DC supplies installed**



**Figure 15 – A6100B 10G Ethernet port close-up - XFPs installed**



**Figure 16 – A6040B 1G Ethernet ports close-up - SFPs installed**



**Figure 17 – RJ45 Ethernet, Console and USB close-up**

CN6000 Series Non-Proprietary Security Policy

Table 3 defines the Physical Ports.

**Table 3    CN6000 Series Physical Ports**

| Port | Location | Purpose |
|---|---|---|
| **RJ-45 Ethernet** | Front Panel (LAN) | Allows secure and authenticated remote management by the selected remote management application. |
| **RJ-45 Ethernet** | Front Panel (AUX) | Auxilliary secure and authenticated remote management by the selected remote management application. |
| **RJ-45 RS-232 Console** | Front Panel | The Serial Console port connects to a local terminal and provides a simple command line interface (CLI) for initialization prior to authentication and operation in the approved mode. This port also allows administrative access and monitoring of operations. User name and password authentication is required to access this port. |
| **USB** | Front Panel | The USB port provides a mechanism for applying approved and properly signed firmware upgrades to the module. |
| **Keypad** | Front Panel | Allows entry of initialization commands. |
| **LCD** | Front Panel | Displays configuration information in response to commands entered via the keypad. Also indicates any operational alarm states. |
| **System LEDs** | Front Panel | Indicate the system state, including secure status, alarms and power. |
| **Port LEDs** | Front Panel | Indicate local and network port status and activity. |
| **Network Port** | Front Panel | The Network Port connects to the public network; access is protected by X.509 certificates. The Network Port is of the same interface type as the Local Port. |
| **CN6040** | | SFP[1] and RJ45 sockets |
| **CN6100** | | XFP[2] sockets |
| **Local Port** | Front Panel | The Local Port connects to the private network; access is protected by X.509 certificates. The Local Port is of the same interface type as the Network Port. |
| **CN6040** | | SFP[1] and RJ45 sockets |
| **CN6100** | | XFP[2] sockets |
| **Emergency Erase button** | Front Panel | The concealed front panel Emergency Erase button can be activated using a paperclip or similar tool and will immediately delete the System Master Key. The Emergency Erase button functions irrespective of the powered state of the module. |
| **Power Connectors** | Rear Panel | Provides AC and/or DC power to the module depending upon which power modules have been installed |
| **Power LEDs** | Rear Panel | Indicates whether power module is ON or OFF. |

Note 1: The SFP sockets are the receptacles for the pluggable SFP transceivers.
Note 2: The XFP sockets are the receptacles for the pluggable XFP transceivers.

## 3.2    CN6000 Series Interfaces

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 18 of 60

CN6000 Series Non-Proprietary Security Policy

**Table 4    Logical Interfaces**

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

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

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

| FIPS 140-2 Logical Interface | CN6000 Series Interface | Physical Port |
|---|---|---|
| Data Input | Private Network Interface | Local  Port |
|  | Public Network Interface | Network Port |
| Data Output | Private Network Interface | Local  Port |
|  | Public Network Interface | Network Port |
| Control Input | Local Console | RJ-45 RS-232 Serial Console |
|  | Keypad & Display | Keypad / LCD |
|  | Remote Management Interface | Management RJ-45 Ethernet Port (LAN) |
|  | Private Network Interface | Local Port |
|  | Public Network Interface | Network Port |
|  | Emergency Erase button | Emergency Erase button |
|  | USB Firmware Upgrade | USB Port |
| Status Output | Local Console | RJ-45 RS-232 Serial Console |
|  | Keypad & Display | Keypad / LCD |
|  | Remote Management Interface | Management RJ-45 Ethernet Port (LAN) |
|  | Private Network Interface | Local Port |
|  | Public Network Interface | Network Port |
|  | LEDs | Front & Rear LEDs |
| Power | Power Switch | Power Connector |

CN6000 Series Encryptors support the FIPS 140-2 Logical Interfaces as outlined in Table 6.

Senetas Corp. Ltd.                    **Version 1.25**                    Page 19 of 60

CN6000 Series Non-Proprietary Security Policy

**Table 6    Interface Support**

| Logical Interface | Support |
|---|---|
| **Data Input &<br>Data Output** | **Local Interface:**<br><br>• Connects to the local (private) network; sends and receives plaintext user data to and from the local network.<br><br>**Network Interface:**<br><br>• Connects to the public network; sends and receives ciphertext user data, via the public network, to and from a far end cryptographic module.<br><br>• Authenticates with the far end cryptographic module(s); sends and receives authentication data and RSA or ECDSA/ECDH key exchange components to and from a far end module.<br><br>The module can be set to bypass allowing it to send and receive plaintext user data for selected connections. |
| **Control Input** | Control Input is provided by the Local Console, Keypad & Display, and the Remote Management Interface as follows:<br><br>• The Keypad supports module initialization prior to authentication and operation in the approved mode. A Crypto Officer sets the IP address for administration by the remote management application; sets the system clock; and loads, in conjunction with the remote management application, the module's certificate.<br><br>• As an alternative to using the Keypad, the Local Console may be used for initialization prior to certification and operation in the approved mode. The Local Console receives control input from a locally connected terminal.<br><br>• Following initialization and authentication, the remote management application can communicate with the module to receive out-of-band control input.<br><br>When configured for in-band management, the Private and Public Network Interfaces may also receive control input. In this mode, the remote management application sends control input by way of the Local or Network Port rather than the RJ-45 Ethernet. |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 20 of 60

CN6000 Series Non-Proprietary Security Policy

| Logical Interface | Support |
|---|---|
| **Status Output** | Status output is provided by the Keypad & Display, LEDs, Local Console and the Remote Management Interface as follows:<br><br>• The Display presents the Crypto Officer with the command data being entered via the Keypad. It also indicates the state of the X.509 certificates.<br><br>• The System LEDs indicate the system and tunnel state as well a combined alarm status covering network and local ports.<br><br>• The Port LEDs indicate the state of the local and network interfaces and the presence of network traffic.<br><br>• As an alternative to using the Keypad & Display, the Local Console may be used for initialization prior to certification and operation in the approved mode. The Local Console may also be used for monitoring some operations; status output is sent to a locally connected terminal.<br><br>• Following initialization and authentication, the module sends out-of-band status output to the remote management application.<br><br>When configured for in-band management, the Private and Public Network Interfaces may also send status output. In this mode, the module status output is sent to the remote management application by way of the Local or Network Port rather than the RJ-45 Ethernet Port. |

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 21 of 60

CN6000 Series Non-Proprietary Security Policy

# 4. Administrative Roles, Services and Authentication

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

The supported roles are summarized in Table 7.

**Table 7    Roles**

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

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

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

**Note: A Crypto Officer should zeroize the module before it is returned to the factory. The module can be zeroized using several methods. When the module is powered on, the module can be zeroized by command or by performing the Erase key press sequence defined in the user manual. An immediate erase can be achieved, powered or un-powered, by depressing the concealed front panel Emergency Erase button, accessed using a "paperclip" or other suitable tool. Refer to Figure 12 for location.**

## 4.1    Identification and Authentication

The module employs Identity-Based Authentication. The module also supports TACACS+ for authentication in FIPS non-Approved mode only. Four operator privilege levels have been defined for use, Administrator, Supervisor,

Operator and Upgrader with access rights as indicated in Table 8. Restricted Administrator privileges are available until the module is "Activated". Activation ensures that the default Administrator password is changed and allows additional user accounts to be created. A user with Administrator privilege can further restrict the available privilege levels to Administrator and Operator by selecting "Simplified" user model from the CLI.

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

Up to 30 user accounts with unique names and passwords may be defined for authorised operators (Administrators, Supervisors Operators and Upgraders) of the module. Operators using the Local Console enter their name and password to authenticate directly with the module. Operators using the remote management application issue commands to the encryptor. Password based authentication is used between the management station and the module to authenticate each user. If the user is authenticated then Diffie-Hellman Key Agreement is employed to establish secure AES SNMPv3 privacy keys allowing the transport of secure messages to and from the module. Commands from the remote management application are individually authenticated to ensure Data Origin Authentication and Data Integrity. Data Origin Authentication, based on the names and passwords, ensures the authenticity of the user claiming to have sent the command. Users employing the module's security functions and cryptographic algorithms, over the Data Input and Output ports, authenticate via certificates that have been generated and signed by a common Certificate Authority (CA). The modules exchange Key Encryption Keys and Data Encryption Keys using RSA-OAEP-256 public key transport in accordance with NIST SP800-56B Rev2 Section 9. Alternatively, ECDH ephemeral key agreement is used for the purpose of establishing DEKs in accordance with NIST SP800-56A Rev3.

Table 8    Authentication Type

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

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

Table 9    Strength of Authentication

| Authentication Mechanism | Strength |
|---|---|
| **Password** | Crypto Officers, Operators, and Upgraders accessing the module CLI, via the Local Console, must authenticate using a password that is at least 8 characters and at most 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 $1/1,000,000$. <br> After three failed authentication attempts via the CLI, the Local Console port access is locked for 3 minutes. With the 3 minute lockout, the possibility of randomly guessing a password in 60 seconds is $3/94^8$ which is less than $1/100,000$. |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 23 of 60

CN6000 Series Non-Proprietary Security Policy

| Authentication Mechanism | Strength |
|---|---|
| | Note: The module also suppresses feedback of authentication data, being entered into the Local Console, by returning * characters. |
| Network User Certificates | Far end modules (Users) authenticate using an RSA authentication certificate based on 2048 bit keys providing 112 bit key size equivalence. Therefore possibility of deriving a private RSA key is $1/2^{112}$ which is far less than 1 in 1,000,000. Alternatively far end modules authenticate using an ECDSA authentication certificate using NIST P-256, P-384 or P-521 may curves which provide 128, 192 and 256 bit key size equivalence respectively. The worst case probability of deriving an ECDSA private key is $1/2^{128}$ which is far less than 1 in 1,000,000. Upon an unsuccessful authentication attempt the secure session establishment mechanism will go into a fault state that takes one minute to clear. This gives a possibility of randomly guessing the authentication key in 60 seconds of $1/2^{112}$ for RSA and $1/2^{128}$ for ECDSA certificates which are both less than 1 in 100,000. |

## 4.2    Roles and Services

CN6000 Series Encryptors support the services listed in the following tables. The tables group the authorized services by the module's defined roles and identify the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

**R** - The item is **read** or referenced by the service.

**W** - The item is **written** or updated by the service.

**E -** The item is **executed** by the service (the item is used as part of a cryptographic function)

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

**N/A** - Not Applicable.

The module's services are described in more detail in the CN6000 Series documentation.

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

Table 10    Operator – Roles and Services

| Crypto Officer | | User | | Authorized Service | Cryptographic Keys and CSPs | Access Type |
|---|---|---|---|---|---|---|
| Admin | Supv | Oper | Upgr | | | |
| ✓ | ✓ | | | Set Real Time Clock | none | N/A |
| ✓ | | | | Load Module Certificate[7] | RSA or ECDSA Public and Private Keys[8], SMK or SMK_CSP | W, R |
| ✓ | | | | Create User Account | Password, SMK or SMK_CSP | W, R |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 24 of 60

CN6000 Series Non-Proprietary Security Policy

| Crypto Officer | | User | | Authorized Service | Cryptographic Keys and CSPs | Access Type |
|---|---|---|---|---|---|---|
| Admin | Supv | Oper | Upgr | | | |
| ✓ | | | | Modify User Account | Password | E, W |
| ✓ | | | | Delete User Account | Password | D |
| ✓ | ✓ | ✓ | ✓ | View User Account | none | N/A |
| ✓ | ✓ | | | Edit Connection Action Table (Bypass)[9] | none | N/A |
| ✓ | ✓ | ✓ | ✓ | View Connection Action Table | none | N/A |
| ✓ | ✓ | ✓ | ✓ | Show Firmware Version | none | N/A |
| ✓ | | | | Clear Audit Trail | Password | W |
| ✓ | ✓ | ✓ | ✓ | View Audit Trail | none | N/A |
| ✓ | | | | Clear Event Log | Password | W |
| ✓ | ✓ | ✓ | ✓ | View Event Log | none | N/A |
| ✓ | ✓ | ✓ | ✓ | View FIPS Mode Status | none | N/A |
| ✓ | | | | Change FIPS Mode Status | Password | W |
| ✓ | ✓ | | | Run Self Test (Reboot Command) | Password | E |
| ✓ | | | ✓ | Install Firmware Upgrade | Password<br>Firmware Upgrade RSA Public Key | E |
| ✓ | | | ✓ | Establish FTPS (TLS) Session | FTPS (TLS) Privacy Keys[3], FTPS (TLS) Private Key, FTPS (TLS) Public Key, FTPS (TLS) HMAC keys, FTPS (TLS) Master Secret[8], SMK or SMK_CSP | R, W, E |
| ✓ | | | ✓ | Establish SFTP (SSH) Session | SFTP (SSH) Privacy Keys[3], SFTP (SSH) Key Exchange Private Keys, SFTP (SSH) Key Exchange Public Keys, SFTP (SSH) HMAC keys, SFTP (SSH) Shared Secret[8], SMK or SMK_CSP | R, W, E |
| ✓ | ✓ | | | Re/Start Secure Connection | AES KEKs[1], SME KDKs[1,5], AES DEKs[1], AES GEKs[6], GDKs[6], SME HMAC key, ECDHE keys, ECDHE Shared Secret[8], SMK or SMK_CSP | W |

Senetas Corp. Ltd.　　　　**Version 1.25**　　　　Page 25 of 60

CN6000 Series Non-Proprietary Security Policy

| Crypto Officer | | User | | Authorized Service | Cryptographic Keys and CSPs | Access Type |
|---|---|---|---|---|---|---|
| Admin | Supv | Oper | Upgr | | | |
| ✓ | | | | Generate X.509v3 Certificate Signing Request | RSA Private Key and RSA Public Key or ECDSA Private Key and ECDH Public Key[8], SMK or SMK_CSP | R, E |
| ✓ | | | | Erase Module – Zeroize (Console Command) | System Master Key and all CSP data stored in non-volatile memory | D |
| ✓ | ✓ | ✓ | ✓ | Establish a Remote Management Session | SNMPv3 Privacy Key[2], SNMPv3 Diffie Hellman Private Keys, SNMPv3 Diffie Hellman Public Keys[8] | R, W, E |
| ✓ | ✓ | ✓ | ✓ | Establish a Remote CLI Session[4] | Remote CLI (SSH) Privacy Keys, Remote CLI (SSH) Key Exchange Private Keys, Remote CLI (SSH) Key Exchange Public Keys, Remote CLI (SSH) HMAC keys[8] | R, W, E |
| ✓ | ✓ | ✓ | ✓ | Establish RESTful HTTPS (TLS Session) | REST (TLS) Privacy Keys[3], REST (TLS) Private Key, REST (TLS) Public Key, REST (TLS) HMAC keys, REST (TLS) Master Secret[8], SMK or SMK_CSP | R, W, E |
| ✓ | | | | KeyVault Sign (X.509v3 Certificate Signing Request) | RSA or ECDSA Private Key[8], SMK or SMK_CSP | R, E |
| ✓ | | | | KeyVault Encrypt | RSA Public Key[8] | R, E |
| ✓ | | | | KeyVault Decrypt | RSA Private Key[8], SMK or SMK_CSP | R, E |
| ✓ | | | | KeyVault DRBG Access | none | N/A |
| ✓ | | | | KeyVault Backup | RSA Private/ Public Key  ECDSA Private/ Public Key  PKCS#12 Password, SMK or SMK_CSP | R, W |
| ✓ | | | | Enable KeySecure | SMK_Local, SMK_Remote | |
| ✓ | | | | KeyVault Restore | RSA Private/ Public Key  ECDSA Private/ Public Key  PKCS#12 Password, SMK or SMK_CSP | R, W |
| ✓ | | | | Generate TIM KDK | TIM Key Derivation Key (KDK) | W |

CN6000 Series Non-Proprietary Security Policy

| Crypto Officer | | User | | Authorized Service | Cryptographic Keys and CSPs | Access Type |
|---|---|---|---|---|---|---|
| Admin | Supv | Oper | Upgr | | | |
| ✓ | | | | Configure KeySecure | KMS (TLS) Privacy Keys[3], KMS (TLS) Private Key, KMS (TLS) Public Key, KMS (TLS) HMAC keys, KMS (TLS) Master Secret[8], SMK_Local, SMK_Mask, SMK_CSP | R, W, E |

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

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

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

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

Note 5:  KDKs are established using Approved RSA-OAEP-256 key transport as per NIST SP-800-56B Rev2 Section 9 and described in Table 13.

Note 6:  GDKs are established using ECDH key agreement.

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

Note 8:  All key material is sourced from the SP-800-90A DRBG and in accordance with IG Section 14.5 the entropy input string, seed and state variables V and C are considered CSPs.

Note 9:  Changing a connection's CI Mode state to Bypass will result in all data transmitted on the connection being sent in plaintext.

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 27 of 60

CN6000 Series Non-Proprietary Security Policy

# 5. Physical Security

CN6000 Series Encryptors employ the following physical security mechanisms:

1. The encryptor is made of commercially available, production grade components meeting commercial specifications for power, temperature, reliability, shock and vibration. All Integrated Circuit (IC) chips have passivation applied to them. The metal enclosure is opaque to the visible spectrum. The ventilation holes on the encryptor's front panel are factory fitted with baffles to obscure visual access and to prevent undetected physical probing inside the enclosure. Attempts to enter the module without removing the cover will cause visible damage to the module, while removing the cover will trigger the tamper circuitry.

2. Access to the internal circuitry is restricted by the use of tamper detection and response circuitry which is operational whether or not power is applied to the module. Attempting to remove the enclosure's cover immediately causes the module to be set into 'Discard' mode and initiates the zeroization of all Keys and CSPs. For further details refer to Section 6.2.

3. Two tamper evident seals are pre-installed (at factory). Both are placed between the top cover and underside of the main enclosure (refer to Figure 18). 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 18 – Factory installed tamper seals**

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

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

Senetas Corp. Ltd.      **Version 1.25**      Page 28 of 60

CN6000 Series Non-Proprietary Security Policy

**Table 11   Physical Security Inspection & Test**

| Security Mechanism | Inspection & Test Guidance | Frequency |
|---|---|---|
| **Tamper Evidence** | Tamper indication is available to all user roles via the alarm mechanism and physical evidence of tampering against the tamper seals.<br><br>The Crypto Officer is responsible for the physical security inspection.<br><br>During normal operation, the Secure LED is illuminated **green**. When the unit is not activated and/or uncertified (i.e. it has no loaded certificate since it is either in the default factory manufactured state or a user erase operation has been executed) or in the tampered state, the Secure LED is illuminated **red** and all traffic is blocked. Inspect the enclosure and tamper evident seals for physical signs of tampering or attempted access to the cryptographic module. | In accordance with the organization's Security Policy. |
| **Tamper Circuit** | The module enters the tampered state when the circuit is triggered. Once in this state, the module blocks all user traffic until the module is re-activated and re-certified. | No direct inspection or test is required; triggering the circuit will block all data flow. |

CN6000 Series Non-Proprietary Security Policy

# 6. Cryptographic Key Management

## 6.1 Cryptographic Keys and CSPs

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

### Table 12   Cryptographic Keys and CSPs

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| AES System Master Key (SMK)[6] | AES-CFB 256-bit key. On initialization, the module generates the System Master Key. This key encrypts the module's RSA Private Key(s) and ECDSA Private Key(s) and the user passwords stored in the configuration flash memory. | Approved Key Generation: FIPS197 SP 800-133 Key Generation using SP 800-90A DRBG | Persistently stored in plaintext in a tamper protected memory device | No | N/A | • Tamper event • Emergency erase button • Erase command |
| Triple-DES System Master Key | 3-key Triple-DES CFB8 192 bit key. The Triple-DES SMK is only used to decrypt CSPs when upgrading from legacy versions of firmware. The CSPs are subsequently re-encrypted using the AES SMK and the Triple-DES System Master Key is destroyed. Triple-DES is no longer used by the module for encryption operations | Approved Key Generation: FIPS197 SP 800-133 Key Generation using SP 800-90A DRBG | Stored in plaintext in a tamper protected memory device | No | N/A | • Destroyed during upgrade process |
| SMK_Local | 256-bit Composite Key When KeySecure is configured the local System Master Key (SMK_local) is generated from the internal DRBG and stored it in tamper protected memory. | Approved Key Generation: FIPS197 SP 800-133 Key Generation using SP 800-90A DRBG | Persistently stored in plaintext in a tamper protected memory device | No | N/A | • Tamper event • Emergency erase button • Erase command |
| SMK_Mask | 256-bit Composite Key When KeySecure is configured the module will obtain a System Master Key mask (SMK_mask) from the external KeySecure server. | External | Stored ephemerally in volatile system memory | No | N/A | • Tamper event • Emergency erase button • Zeroized after use • Power cycle |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 30 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **SMK_CSP** | **AES-CFB 256-bit key** SMK_local and SMK_mask are combined to create SMK_CSP which is used to encrypt and decrypt the module's RSA Private Key(s) and ECDSA Private Key(s) and the user passwords stored in the configuration flash memory. | Created by combining SMK_local and SMK_mask | Stored ephemerally in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Zeroized after use<br>• Power cycle |
| **RSA Private Key(s)** | **2048-bit key.** Generated when the module receives a Load Certificate command from the remote management application. The RSA Private Key(s) are used to authenticate connections with other encryptors and to unwrap master session keys (KDK or GDK) and initial session keys (DEKs) received from far-end encryptors. KeyVault Sign: The RSA Private Key(s) are used to sign X.509v3 Certificate Signing Requests KeyVault Decrypt: The RSA Private Key(s) are used to decrypt externally supplied session keys (KDK, GDK and initial DEKs). | Approved Key Generation: FIPS 186-4 RSA SP 800-133 Key Generation using SP 800-90A DRBG | Persistently stored AES-256 encrypted using the **System Master Key** in non-volatile system memory. | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **RSA Public Key(s)** | **2048-bit key.** Generated when the module receives a Load Certificate command from the remote management application. The RSA Private Key(s) are used to authenticate connections with other encryptors. KeyVault Encrypt: The RSA Public Key(s) are used to encrypt externally supplied session keys (KDK or GDK and initial DEKs). **Note:** The module and the remote management application CM7 will only generate certificates with RSA 2048-bit key size, however It is possible to load a certificate from an external CA with RSA 4096-bit key size. The module certificate will have an RSA 2048-bit key which will be used for key wrapping the KDK, GDK and initial DEKs. | Approved Key Generation: FIPS 186-4 RSA SP 800-133 Key Generation using SP 800-90A DRBG | Persistently stored plain-text in **the Module Certicate(s)** in non-volatile system memory. | Electronic | Plaintext within **X.509 Module Certificate(s)** signed by trusted CA | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **ECDSA Private Key(s)** | **P-256, P-384 or P-521 curve.** Generated when the module receives a Load Certificate command from the remote management application. The ECDSA Private Key(s) are used to authenticate connections with other encryptors. KeyVault Sign: The ECDSA Private Key(s) are used to sign X.509v3 Certificate Signing Requests | Approved Key Generation: 186-4 SP 800-133 Key Generation using SP 800-90A DRBG | Persistently stored AES-256 encrypted using the **System Master Key** in non-volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command |

Senetas Corp. Ltd.          **Version 1.25**          Page 31 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **ECDSA Public Key(s)** | **P-256, P-384 or P-521 curve.** Generated when the module receives a Load Certificate command from the remote management application. The ECDSA Private Key(s) are used to authenticate connections with other encryptors. | Approved Key Generation: 186-4 SP 800-133 Key Generation using SP 800-90A DRBG | Stored persistently in plain-text in **the Module Certicate(s)** in non-volatile system memory. | Electronic | Plaintext within **X.509 Module Certificate(s)** signed by trusted CA | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **ECDH Ephemeral Private Key** | **P-256, P-384 or P-521 curve.** Established during the key agreement process and destroyed once the process is complete. The ECDH Ephemeral Private Key is used to create the shared secret. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in volatile system memory. | No | N/A | • Tamper event<br>• Emergency erase button<br>• Zeroized after session establishment<br>• Power cycle |
| **ECDH Ephemeral Public Key** | **P-256, P-384 or P-521 curve.** Established during the key agreement process and destroyed once the process is complete. The ECDH Ephemeral Private Key is used to create the shared secret. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in volatile system memory. | Electronic | N/A | • Tamper event<br>• Emergency erase button<br>• Zeroized after session establishment<br>• Power cycle |
| **ECDH Shared Secret** | The ECDH Shared Secret is used to derive the Data Encryption Key in point to point sessions or the GEK in group sessions | Established by Approved SP 800-56A Rev3 KAS process | Stored ephemerally in volatile system memory. | Electronic | N/A | • Tamper Event<br>• Emergency erase button<br>• Erase command<br>• Zeroized after session establishment<br>• Power cycle |
| **Module Certificate(s)** | **An X.509 certificate**: is associated with a session in an operational environment. It is produced, upon request from the module, and signed by the Certificate Authority (CA) to establish root trust between encryptors. Once a certificate has been authenticated, Far-end encryptors use the signed RSA Public Key to wrap the initial session keys (KEKs) used to encrypt a session. Alternatively, far end encryptors use the signed ECDSA public key to authenticate messages sent during the ECDH key agreement process. | NA | Persistently stored in plaintext, in non-volatile system memory | Electronic | Plaintext signed by trusted CA | • Tamper event<br>• Emergency erase button<br>• Erase command |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 32 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin<br>Entry/Estab./Gen | Storage | Sourced | Format | |
| **Authentication Password** | **Up to 30 unique Crypto Officers (Administrators, Supervisors) or Users (Operators, Upgraders) may be defined, with associated passwords, within the module.**<br><br>The CLI uses the Authentication Password to authenticate Crypto Officers and Users accessing the system via the Local Console.<br><br>The remote management application requires an authentication password that is used to uniquely authenticate each command to the module. | Manually Entered in plain-text over directly attached serial cable | AES-256-bit encrypted using the system master key. Stored non-volatile system memory. | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **Key Encrypting Key (KEK)** | **AES-CFB 256.**<br><br>For each RSA based session (CI) and EC Multipoint sessions, the AES KEK is derived from the SME KDK using a SP 800-108 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.<br><br>EC point to point connections use ECDH key agreement to generate the DEKs. In this case there is no need for KEKs. | Approved Key Generation:<br><br>Derived from the SME KDK using a SP 800-108 compliant KDF | Stored ephemerally in plaintext, in volatile SDRAM system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 33 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| Data Encrypting Key (DEK) | AES CFB, CTR and GCM, 128-bit or 256-bit keys<br><br>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.<br>In Transport Independent Mode each encryptor uses a single egress DEK to encrypt all secure traffic. Each encryptor maintains 2 egress DEKs one in current use and one stored for the next key update. The egress DEKs are updated every hour. | Generated:<br>FIPS197,<br>SP 800-133 Key Generation using SP 800-90A DRBG<br>or<br>Input using Approved RSA-OAEP-2048 KTS<br>or<br>Established by Approved Key Agreement using ECDH<br>or<br>Derived from a Key Derivation Key using SP 800-108 compliant KDF<br>or<br>Provided by an external KMIP Key Server | Stored ephemerally in plaintext, in volatile SDRAM system memory | Yes | For secure connections assigned to RSA certificates RSA-OAEP-256 KTS is used to transfer the initial DEK to a far-end module. Subsequent DEKs are transferred using AES key wrapping (KEK) authenticated with HMAC-SHA-256.<br><br>For each ECDSA/ECDH based connection (CI) a pair of encryptors use ECDH KAS to establish DEKs. | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| TIM Key Derivation Key (KDK) | The KDK is used to derive the DEKs using a SP 800-108 compliant KDF | FIPS197,<br>SP 800-133 Key Generation using SP 800-90A DRBG and Installed via CM7 | AES-256-bit encrypted using the system master key. Stored non-volatile system memory. | Yes | Transferred via CM7 | • Tamper event<br>• Emergency erase button<br>• Erase command |
| Group Establishment Key (GEK) | AES-CFB256.<br><br>The GEK is used to wrap the group SME KDKs and initial DEKs using AES-256 CFB authenticated with HMAC-SHA-256. | Derived from the GDK using an SP 800-108 compliant KDF | Stored ephemerally in volatile system memory. | Electronic | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| SME HMAC keys | HMAC-SHA-256 with 256-bit key length<br><br>The SME HMAC keys are used to protect the integrity of the AES key wrapped messages between encryptors | Derived from the GDK using an SP 800-108 compliant KDF | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.          **Version 1.25**          Page 34 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin<br><br>Entry/Estab./Gen | Storage | Sourced | Format | |
| **SME KDK** | **256 bit Key Derivation Key**<br>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 | Approved Key Generation:<br><br>186-4<br>SP 800-133 Key Generation using SP 800-90A DRBG<br><br>or<br><br>Established by Approved Key Transport using RSA-OAEP-KTS or AES key wrapping (GEK) authenticated with HMAC-SHA-256 | Stored ephemerally in plaintext, in volatile SDRAM system memory | Yes | Wrapped for transport using the far-end module's public RSA key (RSA-OAEP-256 key transport **or** AES key wrapping authenticated with HMAC-SHA-256) | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **GDK** | **256 bit Group Derivation Key**<br>When a slave joins an ECDSA/ECDH VLAN or multicast group session the key master from the group and the slave use ECDH ephemeral key agreement to establish a GDK that is used to separately derive the GEK and the SME HMAC keys using a SP 800-108 compliant KDF | Established by Approved Key Agreement using ECDH | Stored ephemerally in volatile system memory. | Electronic | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **SNMPv3 Privacy Keys** | **AES-CFB 128 bit Key**<br><br>For each SNMPv3 remote management session, the module uses an AES privacy key established during the Diffie-Hellman key agreement process to secure the control / flow path in the secure connection. | Established by allowed SNMP protocol derivation | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **DRBG Seed** | Used for SP800-90 Hash_DRBG the 440-bit seed (initial V or state) value internally generated from nonce along with entropy input. A hardware based non-deterministic RNG is used for seeding the approved NIST SP 800-90A DRBG. | Internal from ENT (NP) | Stored ephemerally in plaintext in volatile SDRAM system memory | Never exits the module | N/A | • Tamper event<br>• Emergency erase button<br>• Destroyed after use<br>• Power cycle |
| **DRBG Entropy Input and Nonce** | Used for SP800-90 Hash_DRBG as input to the instantiate function. | Internal from ENT (NP) | Stored ephemerally in plaintext in volatile SDRAM system memory | Never exits the module | N/A | • Tamper event<br>• Emergency erase button<br>• Destroyed after u<br>• Power cycle |

Senetas Corp. Ltd.      **Version 1.25**      Page 35 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **DRBG V and C internal state parameters** | The V and C parameters store the internal state of the SP800-90 DRBG. | Internal | Stored ephemerally in plaintext in volatile SDRAM system memory | Never exits the module | N/A | • Tamper event<br>• Emergency erase button<br>• Power cycle |
| **SNMPv3 Diffie Hellman Private Keys** | **2048-bits**<br><br>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. | Established by Diffie-Hellman Key Agreement | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **SNMPv3 Diffie Hellman Public Keys** | **2048-bits**<br><br>The key is created using Oakley group 14 for each SNMPv3 remote SNMPv3 management session to enable agreement of the SNMPv3 privacy key between the module and the management station. | Established by Diffie-Hellman Key Agreement | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **Remote CLI (SSH) Public Key** | **ECDSA P-256, P-384, P-521 curve Key**<br><br>Used to authenticate the remote client with the module. | Loaded electronically onto the module via CM7 or the CLI | Stored persistently in non-volatile system memory. | Electronic | Plaintext | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **Remote CLI (SSH) Key Exchange Private Keys** | **ECDH P-256, P-384, P-521 curve Key**<br><br>The key is created for each remote SSH CLI session to enable agreement of the remote CLI privacy key between the module and the remote client. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **Remote CLI (SSH) Key Exchange Public Keys** | **ECDH P-256, P-384, P-521 curve Key**<br><br>The key is created for each remote SSH CLI session to enable agreement of the remote CLI privacy keys between the module and the remote client. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **Remote CLI (SSH) HMAC keys** | **HMAC-SHA-256 with 256 bit key length**<br>**HMAC-SHA-512 with 512 bit key length**<br><br>The remote CLI (SSH) HMAC keys are used to protect the integrity of the data transmitted across the secure SSH connection. | Internal HMAC operation | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.     **Version 1.25**     Page 36 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
| --- | --- | --- | --- | --- | --- | --- |
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **Remote CLI (SSH) Privacy Keys** | **AES-CTR 128 and 256 bit Key** For each remote CLI session, the module uses an AES privacy key established during the Diffie-Hellman or ECDH key agreement process to secure the control / flow path in the secure SSH connection. | Established by Approved Key Agreement using ECDH | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command<br>• Session termination<br>• Power cycle |
| **SFTP (SSH) Private Key** | **ECDSA P-256, P-384, P-521 curve Key** Used to authenticate the module with the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Persistently stored AES-256 encrypted using the **System Master Key** in non-volatile system memory | No | N/A | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **SFTP (SSH) Public Key** | **ECDSA P-256, P-384, P-521 curve Key** Used to authenticate the module with the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored persistently in non-volatile system memory. | Electronic | Plaintext | • Tamper event<br>• Emergency erase button<br>• Erase command |
| **SFTP (SSH) Key Exchange Private Keys** | **ECDH P-256, P-384, P-521 curve Key** This key is created for each SFTP session to enable agreement of the SFTP privacy key between the module and the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| **SFTP (SSH) Key Exchange Public Keys** | **ECDH P-256, P-384, P-521 curve Key** This key is created for each SFTP session to enable agreement of the SFTP privacy keys between the module and the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.     **Version 1.25**     Page 37 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **SFTP (SSH) HMAC keys** | **HMAC-SHA-256 with 256 bit key length** **HMAC-SHA-512 with 512 bit key length** The SFTP (SSH) HMAC keys are used to protect the integrity of the data transmitted across the secure SSH connection. | Internal HMAC Operation | Stored ephemerally in plaintext, in volatile system memory | No | N/A | • Tamper event • Emergency erase • Erase command (which zeroizes the system master key and deletes the module certificates) • Session termination • Power cycle |
| **SFTP (SSH) Shared Secret** | The SFTP (SSH) Shared Secret is used to derive the SFTP (SSH) privacy keys | Established by allowed SSH protocol derivation. | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event • Emergency erase • Erase command (which zeroizes the system master key and deletes the module certificates) • Session termination • Power cycle |
| **SFTP (SSH) Privacy Keys** | **AES-CTR 128 and 256 bit Key**. For each SFTP session, the module uses an AES privacy key established during the Diffie-Hellman or ECDH key agreement process to secure the control / flow path in the secure SSH connection. | Established by allowed SSH protocol derivation. | All privacy keys are stored in plaintext, in volatile system memory | No | N/A | • Tamper event • Emergency erase • Erase command (which zeroizes the system master key and deletes the module certificates) • Session termination • Power cycle |
| **FTPS (TLS) Private Key** | **ECDSA P-256, P-384, P-521 curve Key** FTPS private key used to authenticate the module with the remote server when using TLS. | Internally generated using SP 800-90A DRBG according to SP 800-133 | AES-256 encrypted format, non-volatile system memory. | No | N/A | • Tamper event • Emergency erase • Erase command (which zeroizes the system master key and deletes the module certificates) |
| **FTPS (TLS) Public Key** | **ECDSA P-256, P-384, P-521 curve Key** FTPS public key used to authenticate the module with the remote server when using TLS. | Electronically input into the module via CM7 | Stored in non-volatile system memory. | Electronic | Plaintext within X.509 certificate self signed by the ftp server or a trusted CA | • Tamper event • Emergency erase • Erase command (which zeroizes the system master key and deletes the module certificates) |

Senetas Corp. Ltd.          **Version 1.25**          Page 38 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| FTPS (TLS) Key Exchange Private Keys | ECDH P-256, P-384, P-521 curve Key<br><br>The secret component of the FTPS (TLS) Key Exchange key pair. The key is created for each FTPS session to enable agreement of the FTPS privacy key between the module and the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| FTPS (TLS) Key Exchange Public Keys | ECDH P-256, P-384, P-521 curve Key<br><br>The public component of the FTPS (SSH) Key Exchange key pair. The key is created for each FTPS session to enable agreement of the FTPS privacy keys between the module and the remote server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| FTPS (TLS) HMAC keys | HMAC-SHA-256 Key length 256 bits<br>HMAC-SHA-384 Key Length 384 bits<br><br>The FTPS (TLS) HMAC keys are used to protect the integrity of the data transmitted across the secure TLS connection. | Internal HMAC Operation | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| FTPS (TLS) Master Secret | The FTPS (TLS) Master Secret is used to derive the FTPS (TLS) privacy keys | Established by allowed TLS protocol derivation. | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.          **Version 1.25**          Page 39 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| FTPS (TLS) Privacy Keys | **AES-CBC or AES-GCM 128 and 256 bit key**<br><br>For each FTPS session, the module uses an AES privacy key established using ECDH to secure the control / flow path in the secure TLS connection. | Established by allowed TLS protocol derivation. | All privacy keys are stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| KMS (TLS) Private Key | **RSA 2048-bits or ECDSA P-256, P384, P-521 curve Key**<br><br>KMS private key used to authenticate the module with the remote key server when using TLS. RSA keys are also used for key transport. | Internally generated using SP 800-90A DRBG according to SP 800-133 | AES-256 encrypted format, non-volatile system memory. | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates) |
| KMS (TLS) Public Key | **RSA 2048-bits or ECDSA P-256, P384, P-521 curve Key**<br><br>KMS public key used to authenticate the module with the remote key server when using TLS. RSA keys are also used for key transport. | Electronically input into the module via CM7 | Stored in non-volatile system memory. | Electronic | Plaintext within X.509 certificate self signed by the ftp server or a trusted CA | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• |
| KMS (TLS) Key Exchange Private Keys | **ECDH P-256, P-384, P-521 curve Key**<br><br>The secret component of the KMS (TLS) Key Exchange key pair. The key is created for each KMS session to enable agreement of the KMS privacy key between the module and the remote key server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| KMS (TLS) Key Exchange Public Keys | **ECDH P-256, P-384, P-521 curve Key**<br><br>The public component of the KMS (TLS) Key Exchange key pair. The key is created for each KMS session to enable agreement of the KMS privacy keys between the module and the remote key server. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.          **Version 1.25**          Page 40 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **KMS (TLS) HMAC keys** | HMAC-SHA-256 Key length 256 bits<br>HMAC-SHA-384 Key Length 384 bits<br><br>The KMS (TLS) HMAC keys are used to protect the integrity of the data transmitted across the secure TLS connection. | Internal HMAC Operation | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| **KMS(TLS) Master Secret** | The KMS (TLS) Master Secret is used to derive the KMS (TLS) privacy keys | Established by allowed TLS protocol derivation. | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| **KMS (TLS) Privacy Keys** | **AES-CBC or AES-GCM 128 and 256 bit key**<br><br>For each KMS session, the module uses an AES privacy key established using ECDH to secure the control / flow path in the secure TLS connection. | Established by allowed TLS protocol derivation. | All privacy keys are stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| **REST (TLS) Private Key** | **ECDSA P-256, P-384, P-521 curve Key**<br><br>RESTful interface private key used to authenticate the module with the remote RESTful client using TLS. | Internally generated using SP 800-90A DRBG according to SP 800-133 | AES-256 encrypted format, non-volatile system memory. | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates) |
| **REST (TLS) Public Key** | **ECDSA P-256, P-384, P-521 curve Key**<br><br>RESTful interface public key used to authenticate the module with the remote RESTful client using TLS. | Electronically input into the module via CM7 | Stored in non-volatile system memory. | Electronic | Plaintext within X.509 certificate self signed by the ftp server or a trusted CA | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• |

Senetas Corp. Ltd.          **Version 1.25**          Page 41 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| REST (TLS) Key Exchange Private Keys | ECDH P-256, P-384, P-521 curve Key<br><br>The secret component of the Restful interface (TLS) Key Exchange key pair. The key is created for each Restful interface session to enable agreement of the Restful interface privacy key between the module and the remote client. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| REST (TLS) Key Exchange Public Keys | ECDH P-256, P-384, P-521 curve Key<br><br>The public component of the Restful interface (TLS) Key Exchange key pair. The key is created for each Restful interface session to enable agreement of the Restful interface privacy keys between the module and the remote client. | Internally generated using SP 800-90A DRBG according to SP 800-133 | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| REST (TLS) HMAC keys | HMAC-SHA-256 Key length 256 bits<br>HMAC-SHA-384 Key Length 384 bits<br><br>The Restful interface (TLS) HMAC keys are used to protect the integrity of the data transmitted across the secure TLS connection. | Internal HMAC Operation | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |
| REST (TLS) Master Secret | The Restful interface (TLS) Master Secret is used to derive the Restful interface (TLS) privacy keys | Established by allowed TLS protocol derivation. | Stored in plaintext, in volatile system memory | No | N/A | • Tamper event<br>• Emergency erase<br>• Erase command (which zeroizes the system master key and deletes the module certificates)<br>• Session termination<br>• Power cycle |

Senetas Corp. Ltd.          **Version 1.25**          Page 42 of 60

CN6000 Series Non-Proprietary Security Policy

| Key/CSP | Key Type and Use | Key/CSP | | Key/CSP Output | | Key/CSP Destruction |
|---|---|---|---|---|---|---|
| | | Origin Entry/Estab./Gen | Storage | Sourced | Format | |
| **REST (TLS) Privacy Keys** | **AES-CBC or AES-GCM 128 and 256 bit key** <br><br> For each Restful interface session, the module uses an AES privacy key established using ECDH to secure the control / flow path in the secure TLS connection. | Established by allowed TLS protocol derivation. | All privacy keys are stored in plaintext, in volatile system memory | No | N/A | • Tamper event <br> • Emergency erase <br> • Erase command (which zeroizes the system master key and deletes the module certificates) <br> • Session termination <br> • Power cycle |
| **Firmware Upgrade RSA Public Key** | **2048-bit key** <br><br> 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. | Pre-Loaded at Factory | Stored in non-volatile system memory. | Electronic | Plaintext | N/A. This public key is embedded in the firmware. |

Note 1: While the certificates, maintained within the module, are listed as CSPs, they contain only public information.
Note 2: As per SP 800-133, all random data including cryptographic Key material is sourced unmodified from the NIST SP800-90A DRBG as required.
Note 3: Switching modes or selecting the front panel key press erase sequence or pressing the concealed Emergency Erase button initiates a module Erase resulting in the destruction of this Key/CSP.
Note 4: The ECDH key agreement methodology as implemented in the module provides between 128 and 256 bits of encryption strength.
Note 5: The services above which utilize key establishment methods, shall be configured to use only the cipher suites labelled as "approved" when operating in the approved mode. Failure to utilize the approved cipher suites as per Table 17 and Table 18 of this security policy, will place the modules into a non-approved mode of operation.
Note 6: The system Master Key is never used for key wrapping for transporting keys.
Note 7: The module generates entropy in 256 bit blocks. Each 256 bit block contains full entropy.

Senetas Corp. Ltd.          **Version 1.25**          Page 43 of 60

CN6000 Series Non-Proprietary Security Policy

## 6.2 Key and CSP zeroization

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

Crypto Officer initiated zeroization will occur immediately when the:

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

Automatic zeroization will occur immediately when the module is:

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

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

### 6.2.1 Zeroization sequence

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

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

### 6.2.2 Erase command and key press sequence

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

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

### 6.2.3 Approved mode of operation

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 44 of 60

CN6000 Series Non-Proprietary Security Policy

### 6.2.4  Tamper initiated zeroization

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

The tamper initiated zeroization process achieves the following:

1. Zeroization of the System Master Key (SMK) rendering the RSA and ECDSA Private Keys, TIM KDK, User passwords and other CSPs indecipherable. Zeroization of the SMK occurs irrespective of the powered state of the module.

2. When powered on and the Tamper Circuit is triggered, the module will automatically:

   a. Set the encryption mode for each session (CI)  to DISCARD ensuring no user data is output from the module,

   b. Log the tamper event to the Audit Log,

   c. Set the System, Secure and Alarm LEDs to flash RED on the front panel and herald the tamper event via the internal speaker,

   d. Initiate the Zeroization sequence zeroizing all Session Keys (DEKs) and CSPs in volatile system memory and non-volatile Configuration and User account data,

   e. REBOOT the module.

3. When powered off and the Tamper Circuit is triggered, there are no Session Keys (DEKs) or CSPs in system volatile memory to be zeroized however upon re-powering the module, the zeroized System Master Key will indicate that the system has been tampered. The module will:

   a. Log the tamper event to the Audit log,

   b. Initiate the Zeroization sequence,

   c. Continue to the BOOT, returning the module to the un-Activated factory default state.

4. When the BOOT sequence has completed the module will have:

   a. Generated a new System Master Key,

   b. Re-created the default administration account,

   c. Set the encryption mode to DISCARD,

   d. Entered the factory default state ready for Configuration (as described in Section 8.3 below).

### 6.2.5  "Emergency" Erase

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

### 6.2.6  KeySecure Connector integration

The CN6000 series of 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 remote System Master Key mask (SMK_mask) from the external KeySecure server. When the encryptor needs to encrypt or decrypt a CSP it will retrieve SMK_local and SMK_mask and combine them to create SMK_csp which is used to perform the crypto operation.

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

### 6.3  Data privacy

To ensure user data privacy the module prevents data output during system initialization. No data is output until the module is successfully authenticated (activated) and the module certificate has been properly loaded. Following

Senetas Corp. Ltd.                    **Version 1.25**                    Page 45 of 60

CN6000 Series Non-Proprietary Security Policy

system initialization, the module prevents data output during the self tests associated with a power cycle or reboot event. No data is output until all self tests have completed successfully. The module also prevents data output during and after zeroization of data plane cryptographic keys and CSPs; zeroization occurs when the tamper circuit is triggered. In addition, the system's underlying operational environment logically separates key management functions and CSP data from the data plane.

## 6.4    Cryptographic Algorithms

CN6000 Series Encryptors employ the following approved cryptographic algorithms.

Table 13 lists approved software algorithms that are common to the CN6000 Series. These algorithms are used during the establishment of secure connections, for management services (SNMP, TLS and SSH) and to generate and encrypt CSPs.

**Table 13   FIPS Approved Algorithms – CN6000 Series Common Crypto Library**

| Algorithm Type | Algorithm | FIPS Validation Certificate | |
|---|---|---|---|
| **CN6000 Series Common Crypto Library** | | | **CN6040 / CN6100** |
| **Symmetric Key** | **Triple-DES** TCFB8[1] (d; KO 1) | Triple-DES A1583 | |
| | **AES** CFB128 (e/d; 128,256) | AES A1583 | |
| | **AES** CTR (int only; 128, 256) | AES A1583 | |
| | **AES** ECB[2] (e/d; 128, 256) | AES A1583 | |
| | **AES** CBC (e/d; 128,256) | AES A1583 | |
| | **AES** GCM (e/d; 128,256 Internal IV, AAD=0 to 248) | AES A1583 | |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 46 of 60

CN6000 Series Non-Proprietary Security Policy

| | | | |
|---|---|---|---|
| **Asymmetric Key** | **RSA**<br>FIPS186-4:<br>KeyGen[3]; MOD: 2048<br>ALG[RSASSA-PKCS1_V1_5];<br>SigGen; MOD: 2048 SHS: SHA-256<br>SigVer[4]; MOD: 2048 SHS: SHA-256,<br>      SHA-384 and SHA-512<br>      MOD: 4096[5] SHS: SHA-256,<br>      SHA-384 and SHA-512 | RSA A1583 | |
| | **ECDSA**<br>FIPS186-4:<br>PKG: P-256, P-384 and P-521 curves<br>PKV: P-256, P-384 and P-521 curves<br>SigGen P-256 (SHA-256), P-384 (SHA-384) and P-521 (SHA-512) curves<br>SigVer P-256 (SHA-256), P-384 (SHA-384) and P-521 (SHA-512) curves | ECDSA A1583 | |
| | **KAS-ECC**<br>Elliptic Curve Diffie-Hellman (Cofactor) Ephemeral Unified Model key agreement using NIST P-256, P-384 and P-521 curves[10] are supported and SHA-256, SHA-384 and SHA-512 (respectively) are used for key derivation in accordance with SP800-56A Rev3 | KAS-ECC A1583 | |
| | **KAS-FFC**<br>Diffie-Hellman dhEphem key agreement using MODP-2048 bit Oakley Group 14[11] using SHA-256 for key derivation in accordance with SP800-56A Rev3 | KAS-FFC A1583 | |
| **Hashing** | **SHA1/2**<br>SHA-1[6] (BYTE only)<br>SHA-256 (BYTE only)<br>SHA-384 (BYTE only)<br>SHA-512 (BYTE only)<br>**SHA3**<br>SHA3-256 (BYTE only) | SHS A1583 | |
| **HMAC** | HMAC-SHA-1[7.] (Key Sizes Ranges Tested: KS<BS)<br>HMAC-SHA-256 (Key Sizes Ranges Tested: KS<BS)<br>HMAC-SHA-384 (Key Sizes Ranges Tested: KS<BS)<br>HMAC-SHA-512 (Key Sizes Ranges Tested: KS<BS) | HMAC A1583 | |

| | | | | |
|---|---|---|---|---|
| **DRBG** | NIST SP800-90A<br>Hash_Based DRBG: [ Prediction Resistance Tested: Not Enabled (SHA-256) ] | | DRBG A1583 | |
| **KBKDF** | NIST SP 800-108 Counter based KDF using HMAC-SHA-256 | | KBKDF A1583 | |
| **CKG** | SP800-133 – sections 5.1 & 5.2 | Asymmetric key generation using unmodified DRBG output | Vendor Affirmed | |
| | SP800-133 – section 6.1 | Direct generation of symmetric key using unmodified DRBG output | Vendor Affirmed | |
| | SP800-133 – section 6.2 | Distribution of generated symmetric key (see KTS) | Vendor Affirmed | |
| | SP800-133 – section 6.3 | Symmetric keys generated using ECDH key agreement in accordance with SP 800-56A Rev3 | Vendor Affirmed | |
| **KTS-RSA** | NIST SP800-56B Rev2 RSA-OAEP-256 Key Transport[8] | | KTS-RSA A1583 | |
| **KTS** | AES-256 CFB key wrapping authenticated with HMAC-SHA-256 | | AES A1583<br>HMAC A1583 | |

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

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

Note 3: The module does not generate RSA keys < 2048 for use in X.509v3 certificates in accordance with NIST SP800-131A.

Note 4: Only RSA 2048 signature verification using SHA-256 is approved.

Note 5: The module and the remote management application CM7 will only generate certificates with RSA 2048-bit key size. It is possible to load a certificate from an external CA with RSA 4096-bit key size, although the encryptor certificate will have an RSA 2048-bit key which will be used for key wrapping the KEKs.

Note 6: The module does not support the use of SHA-1 for X.509v3 certificate digital signatures in line with SP800-131A.

Note 7: HMAC keys < 112 bits are non-compliant in line with SP800-131A. HMAC keys for SSL and TLS are a minimum of 160 bits.

Note 8: Approved RSA-OAEP-256 key transport as per NIST SP-800-56B Rev2 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 9: AES-256 key wrapping provides 256 bit 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 10: 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. Only the use of P-521 will ensure that the established key maintains the full 256 bits of encryption strength.

Note 11: 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.

**TLS AES-GCM Key and IV generation:**

- The module conforms to TLSv1.2 GCM cipher suites as specified in SP 800-52 Rev 1, 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.
- The IV is 96 bits in length and is internally generated randomly using an Approved DRBG in compliance with Section 8.2.2 of NIST SP 800-38D.

Table 14 lists approved firmware algorithms that are specific to the CN6040 and CN6100 hardware versions. These AES implementations are used to encrypt/decrypt data plane traffic.

**Table 14   FIPS Approved Algorithms – CN6000 Series Firmware Algorithms**

| Algorithm Type | Algorithm | FIPS Validation Certificate | Target Model Notes |
|---|---|---|---|
| **CN6040 Module Version 1.9 – 1G Ethernet Mode** | | | **Ethernet Mode** Selectable line rate of: 10/100/1000 Mbps Model number /description: A6040B 1G Ethernet Encryptor |
| **Symmetric Key** | **AES** CFB128 (e/d; 128, 256) | AES A1569 | |
| | **AES** CTR (int only; 128, 256) | AES A1569 | |
| | **AES** ECB (e; 128, 256) | AES A1569 | |
| | **AES** GCM (e/d; 128, 256; Internal IV$^2$, AAD=112 to 688) | AES A1569 | |
| **CN6100 Module Version 1.10 – 10G Ethernet Mode** | | | **Ethernet Mode** Line rate: 10 Gbps Model number /description: A6100B 10G Ethernet Encryptor |
| **Symmetric Key** | **AES** CTR (int only; 128, 256) | AES A1567 | |
| | **AES** ECB (e; 128, 256) | AES A1567 | |
| | **AES** GCM ( e/d; 128, 256; Internal IV$^2$, AAD=112 to 688) | AES A1567 | |
| **CN6100 Module Version 1.10 – 10G Ethernet TIM Mode** | | | **Ethernet Mode** Line rate: 10 Gbps Model number /description: A6100B 10G Ethernet Encryptor |
| **Symmetric Key** | **AES** CTR (int only; 128, 256) | AES A1568 | |
| | **AES** ECB (e; 128, 256) | AES A1568 | |
| | **AES** GCM ( e/d; 128, 256; Internal IV$^2$, AAD=112 to 688) | AES A1568 | |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 49 of 60

CN6000 Series Non-Proprietary Security Policy

Note 1: The IV is 96 bits in length and is Internally generated deterministically in compliance with Section 8.2.1 of NIST SP 800-38D

## 6.5 Entropy

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

### Table 15   Entropy

| Algorithm Type | Algorithm | FIPS Validation Certificate | Models |
|---|---|---|---|
| | | | **CN6040/ CN6100** |
| **RNG** | SP 800-90B Random Number Generator | ENT (NP) | |

## 6.6 Key Derivation Functions

CN6000 Series Encryptors employ the following application-specific Key Derivation Functions (KDFs). Table 16 lists the KDFs.

### Table 16   FIPS Approved KDF

| KDF | Hash Algorithm | FIPS Validation Certificate | Target Model Notes |
|---|---|---|---|
| **CN6000 Series Common Crypto Library** | | | **CN6040 / CN6100** |
| SNMP Privacy and Authentication Key | SHA-1 | CVL (Cert. A1583) | No parts of the SNMP protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP |
| TLS (version 1.2) | SHA-256 SHA-384 | CVL (Cert. A1583) | No parts of the TLS protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP |
| SSH | SHA-1 SHA-256 SHA-384 SHA-512 | CVL (Cert. A1583) | No parts of the SSH protocol, other than the KDF, have been reviewed or tested by the CAVP and CMVP |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 50 of 60

CN6000 Series Non-Proprietary Security Policy

**Table 17   TLS (version 1.2) Cryptographic Algorithms. TLS is used for FTPS (firmware upgrades), RESTful interface and KMS (KeySecure)**

| 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 1.1.0l
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 NIST SP 800-38D


**Table 18   SSH (for Remote CLI and SFTP) Cryptographic Algorithms**

| Algorithm Type | Algorithm |
|---|---|
| Authentication | ECDSA[1] |
| Key Exchange | ECDH[1] |
| Symmetric Encryption | AES-256-CTR |
|  | AES-128-CTR |
|  | AES-128-GCM |
|  | AES-256-GCM |
| 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.

**Note: Please refer to Table 20 in section 8.4 for details on non-Approved algorithms in non-Approved mode of operation.**

Senetas Corp. Ltd.          **Version 1.25**          Page 51 of 60

CN6000 Series Non-Proprietary Security Policy

# 7. Self Tests

CN6000 Series cryptographic modules perform both power-up and conditional self tests to verify the integrity and correct operational functioning of the encryptor. Any failure of a self test will cause the module to transition to an error state and block all traffic on the data ports. Upon entering an error state an operator can attempt to clear the state by restarting the module. If the state cannot be cleared the module must be returned to the manufacturer. Table 19 summarizes the module's self tests.

The design of the CN6000 Series cryptographic modules ensures that all data output, via the data output interface, is inhibited whenever the module is in a self-test condition. Status information displaying the results of the self tests is allowed from the status output interface. No CSPs, plaintext data, or other information, that if misused could lead to a compromise, is passed to the status output interface.

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

**Table 19 Self Tests**

**Table Legend**

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

| Self Test | Description | Fault |
|---|---|---|
| **Mandatory Tests** | **Performed at power-up and on demand** | |
| **Known Answer Tests** | Each cryptographic algorithm, employed by the encryptor, is tested using a "Known Answer Test" to verify the operation of the function.CN6000 Series KATs are divided into four distinct modules which correspond to the common modules listed in table 13 and firmware modules listed in table 14. | |
| CN6000 Series Common Crypto Library | The following CN6000 Series Common Crypto Library algorithms are tested: AES128 CFB encrypt, AES128 CFB decrypt, AES256 CFB encrypt, AES256 CFB decrypt, AES-GCM-128 encrypt, AES-GCM-128 decrypt, AES-GCM-256 encrypt, AES-GCM-256 decrypt,Triple-DES168 encrypt, Triple-DES168 decrypt, SHA-1, SHA-256, SHA-384, SHA-512, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, KDF CTR HMAC-SHA256, RSA2048 encrypt, RSA2048 decrypt, RSA4096 encrypt, RSA4096 decrypt, RSA-OAEP-SHA-256 2048 encrypt, RSA-OAEP-SHA-256 2048 decrypt, ECDSA P-256, P-384, and P-521 (Sign and Verify and KAT), ECDH P-256, P-384, and P-521 (primitive KAT), SP 800-90A DRBG KAT, Statistical, Instantiate, Reseed, | Halt |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 52 of 60

CN6000 Series Non-Proprietary Security Policy

| Self Test | Description | Fault |
|---|---|---|
| | Generate and Un-instantiate tests, ECDH (Cofactor) Ephemeral Unified Model SP800-56Ar3, DH dhEphem 2048 MODP group SP800-56Ar3. | |
| | Each of the AES firmware modules are tested at power-up. | |
| CN6040 1G Ethernet | AES CFB (e/d; 128, 256), CTR (e; 128, 256), GCM (e/d; 128, 256) | Halt |
| CN6100 10G Ethernet | AES CTR (e/d; 128, 256), GCM (e/d; 128, 256) | Halt |
| CN6100 TIM 1G Ethernet | AES CTR (e/d; 128, 256), GCM (e/d; 128, 256) | Halt |
| **Firmware Integrity Test** | An Error Detection Code (32-byte SHA-256 hash) is used to verify the integrity of all components within the cryptographic firmware when the module is powered up. <br><br> Upon any file error the system will enter a Secure shutdown state and Halt ("Secure Halt") | Halt |
| **Bypass Test** | CN6000 Series modules support alternating between Bypass, Discard and Encrypt modes (which can be seen from the management interface). <br><br> The configuration files that control the bypass/discard and encrypt settings are integrity checked using a stored checksum (32 bit CRC). On power-up the module calculates a fresh checksum for all configuration files and compares each to the stored values. Upon a mismatch an error is flagged. The error condition will result in a recreation of the configuration file with the factory default settings. Factory default settings are to fail safe, setting policy to Discard. An audit message is entered to reflect the re-initialisation. <br><br> Any user change (crypto officer) to or from encrypt, bypass or discard shall cause an audit log entry. | Erase |
| **ENT (NP) Start-up Health Test** | The ENT (NP) is tested at start-up using adaptive proportion and repeat count tests compliant with SP800-90B section 4. | |

| Critical Functions | Performed at power-up | |
|---|---|---|
| **Battery** | The battery voltage is tested to determine if it is critically low. This test is guaranteed to fail prior to the battery voltage falling below the minimum specified data retention voltage for the associated battery-backed components. If this test fails, the battery low alarm condition is raised. The module continues to operate however it is advisable that the battery be replaced immediately. The battery is located in the removable fan tray and can be ordered from the module's supplier. | Alarm |

Senetas Corp. Ltd.                    **Version 1.25**                    Page 53 of 60

CN6000 Series Non-Proprietary Security Policy

| Self Test | Description | Fault |
|---|---|---|
| | Battery alarm indication is available to all user roles via the alarm mechanism. | |
| **Real Time Clock / Tamper Memory** | The Real Time Clock (RTC) oscillator is checked at start-up and the Tamper memory is examined for evidence of a Tamper Condition. | Halt |
| **Conditional Tests** | **Performed, as needed, during operation** | |
| **Bypass Test** | The module supports alternating between Bypass, Discard and Encrypt modes (which can be seen from the management interface). The configuration files that control the bypass/discard and encrypt settings are integrity checked using a stored checksum (32 bit CRC).  Conditional bypass tests are enforced by checking the CRC during each process initialisation that memory maps specific configuration data. If the CRC is valid, the process continues execution with that data, otherwise a re-initialisation is executed to failsafe values. Once running, a process will update the relevant configuration data when required, recalculating and storing the new CRC value. | Erase |
| **Pair-wise Consistency** | RSA Public and Private keys are used for the calculation and verification of digital signatures and for key transport. These keys are tested for consistency, based on their purpose, at the time they are used. RSA wrapping keys are tested by an encrypt/decrypt pair-wise consistency test; signature keys are tested by a sign/verify pair-wise consistency test.<br><br>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. | Halt |
| **Firmware Load** | When a new firmware image file is generated by the vendor, the file is encrypted and then signed with the firmware upgrade RSA private key. When any firmware load is applied to the encryptor in the field, the module verifies the authenticity of the firmware image file using its copy of the firmware upgrade RSA public key. Only firmware loads with a valid and verified firmware upgrade RSA signature are accepted. | Error |
| **CRNGT for the ENT (NP) and DRBG** | The ENT (NP) is continuously tested using adaptive proportion and repeat count tests compliant with SP800-90B section 4.4.<br><br>The DRBG is continuously tested according to FIPS140-2 (section 4.9.2). | Reboot |

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

Senetas Corp. Ltd.          **Version 1.25**          Page 54 of 60

CN6000 Series Non-Proprietary Security Policy

CN6000 Series Non-Proprietary Security Policy

# 8. Crypto-Officer and User Guidance

This section provides information for Crypto Officers to install, configure and operate the CN6000 Series Encryptors in FIPS mode.

As outlined in this Security Policy, Crypto Officers (more specifically, Administrators and Supervisors) are the only administrators/operators that can make configuration changes or modify the system settings. The Crypto Officer is responsible for the physical security inspection.

The CN6000 Series is designed to operate in either a FIPS approved mode or a non-FIPS approved mode. The operator can query the FIPS status (operating mode) of a module, and authorized operators may change the FIPS mode of operation. The FIPS status can be queried from the Local Console via the CLI or remotely via the remote management application.

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

**Note: Non-FIPS mode of operation is provided for interoperability with legacy systems. The module's factory default state (prior to commissioning as outlined in section 8.3) for the FIPS configuration setting is Enabled. The CN6000 Series must be explicitly configured to operate in a non-FIPS approved mode.**

The console command is:

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

```
CN6100> fips on

FIPS mode enabled
```

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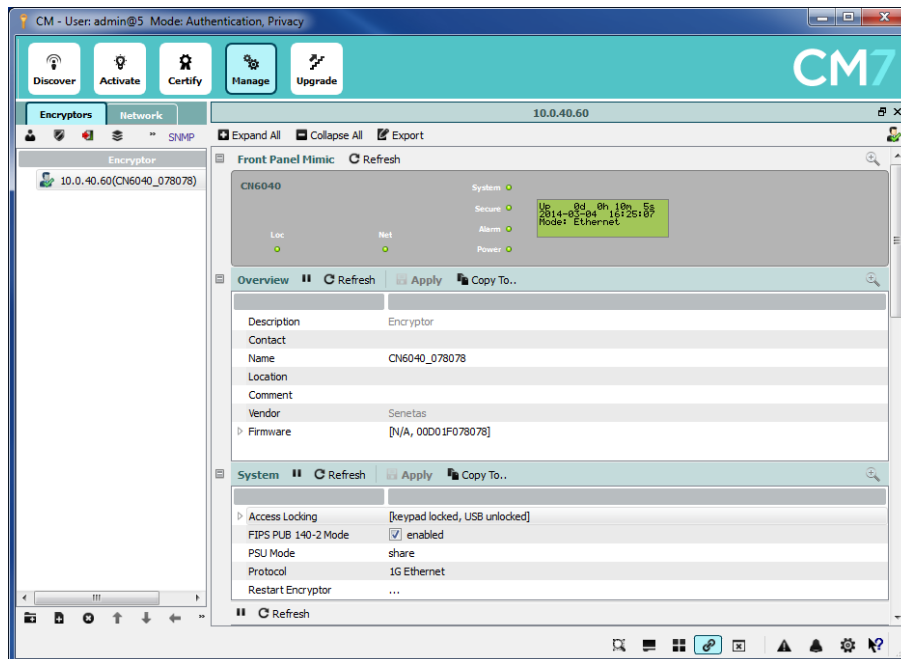


**Figure 19 – FIPS Approved and non-Approved mode selection**

**Note: Read all of the instructions in this section before installing, configuring, and operating the CN6000 Series Encryptors.**

Senetas Corp. Ltd.                    Version 1.25                    Page 56 of 60

CN6000 Series Non-Proprietary Security Policy

## 8.1 Delivery

Before the shipment proceeds a serial number is allocated for the ordered module. Prior to the module shipping, a Shipping Advice form listing the purchase order number, the model number, the serial number and date of shipment is sent to the purchaser. When the module is delivered, the CO can verify that the model and serial numbers on the outside of the packaging, the model and serial numbers attached to the encryptor itself, and the numbers listed on the Shipping Advice form, all match. The CO can also verify that the encryptor has not been modified by examining the tamper evident seal on the outside of the unit. If the seal is broken, then the integrity of the encryptor cannot be assured and the supplier should be informed immediately.

Upon receipt of a CN6000 Series Encryptor, the following steps should be undertaken:

1. Inspect the shipping label as well as the label on the bottom of the system to ensure it is the correct FIPS-approved version of the hardware.

2. Inspect the encryptor for signs of tampering. Check that the tamper evident tape and the covers of the device do not show any signs of tampering. If tampering is detected, return the device to the manufacturer.

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

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

## 8.2 Location

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

Always maintain and operate the CN6000 Series Encryptor in a protected/secure environment. If it is configured in a staging area, and then relocated to its operational location, never leave the unit unsecured and unattended.

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

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

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

## 8.3 Configuration – FIPS140-Approved mode

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

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

1. Power on the unit.

   The system boot-up sequence is entered each time the module is powered on and after a firmware restart. The CN6000 Series Encryptor automatically completes its self tests and verifies the authenticity of its firmware as part of the initialization process. The results of these tests are reported on the front panel LCD and are also logged in the system audit log.

   If errors are detected during the diagnostic phase, the firmware will not complete the power up sequence but will instead enter a Secure shutdown state and Halt ("Secure Halt"). If this occurs the first time power is applied or any time in the future, the module will notify the CO that a persistent (hard) error has occurred and that the module must be returned for inspection and repair.

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

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

4. **Activate** the cryptographic module.

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

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

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

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

   CN6000 Series cryptographic modules support X.509v3 Certificate Signing Requests (CSRs) and will accept certificates signed by the remote management application CM7 (when acting as a CA) as well as certificates signed by External CAs. In both cases each CN6000 Series cryptographic module supplies upon request an X.509v3 CSR containing the module's details and either a 2048 bit Public RSA key or an ECDSA Public key using NIST P-256, P-384 or P-521 curves.

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

   After an X.509 certificate has been installed into CN6000 Series module the administrator can create supervisor and operator accounts.

   At this point the CN6000 Series Encryptor is able to encrypt in accordance with the configured security policy; the ENT key on the front panel is disabled; and the default factory account has been removed.

6. Ensure the encryptor is in FIPS 140-2 mode (default setting) via the Senetas CM7 remote management applications' **Management-Access** tab. See Figure 19 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, VLAN or ISID mode) with Sender ID (SID) enabled the user must set a unique SID between 1 and 512 for each encryptor within the Multipoint group. Failure to do so will place the module in non-approved mode.

8. Configure the security policy to enable encrypted tunnels with other CN6000 Series modules.

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

Senetas Corp. Ltd.          **Version 1.25**          Page 58 of 60

CN6000 Series Non-Proprietary Security Policy

## 8.4    Configuration - Non-Approved Mode

The CN6000 Series is capable of providing a number of non-approved services in order to support legacy functions such as SNMPv3 without privacy enabled and to provide remote AAA support, TACACS+ and other services.

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

Configuring the CN6000 Series into non-Approved mode of operation can be achieved using the CM7 remote management application or the local console via CLI. Once the change is affected the module will automatically erase and restart:

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

    – OR -

2.  Login via the front panel management console and execute the console command e.g. *"CN6100 Encryptor> fips off"*. See Figure 19 for details.


**Table 20    Non-Approved Mode Services**

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

Note 1: OpenSSL version 1.1.0l
Note 2: TACACS+ uses MD5

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

Senetas Corp. Ltd.                    **Version 1.25**                    Page 59 of 60

CN6000 Series Non-Proprietary Security Policy

# 9.  Mitigation of Other Attacks

The module 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.

## 9.1  TRANSEC

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

A TRANSEC enabled module exhibits the following encryption characteristics:

- Generates and transmits fixed size encrypted Ethernet frames at a constant frame rate from the WAN facing network port.

- Encrypts the entire Ethernet frame received on the local port so that no MAC addresses, other header information or payload data is exposed.

- The rate of the transmitted Ethernet frame is constant and independent of the received plaintext traffic rate from the local port.

- In the absence of user data from the local port the TRANSEC encryptor module fills the transmitted frames with pseudo random or encrypted data such that it cannot be distinguished from encrypted user data.

- TRANSEC encryptor modules default to decrypting traffic received on their network interface and discard all introduced traffic that is not 'real' user data.

Senetas Corp. Ltd.                    **Version 1.25**                    Page 60 of 60

CN6000 Series Non-Proprietary Security Policy