Senetas

Distributed by Thales

CN 4000/6000 Series Ethernet Encryptors v5.5.0

Security Target

Version 1.4

March 2025

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Description
0.1	July 2022	Initial Draft
0.2	22 July 2022	Draft for Senetas input.
0.3	29 July 2022	2nd Draft for iteration.
0.4	2 Sep 2022	3rd Draft for iteration.
0.5	12 Oct 2022	Final draft for review.
0.6	1 Nov 2022	Release for evaluation.
0.7	16 Feb 2023	Address OR01
0.8	23 Oct 2023	Address CB OR.
1.0	8 Dec 2023	Address CB OR.
1.1	14 Feb 2024	Updated User Guidance. Updated operational environment.
1.2	20 June 2024	Misc. updates.
1.3	4 March 2025	Updated Build Number.
1.4	21 March 2025	Removed CLI ambiguity.

Table of Contents

1 Introduction 5

1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 5

2 TOE Description 8

2.1 Type 8
2.2 Usage 8
2.3 Logical Scope 11
2.4 Physical Scope 12

3 Security Problem Definition 16

3.1 Threats 16
3.2 Assumptions 16
3.3 Organizational Security Policies 16

4 Security Objectives 17

4.1 Objectives for the Operational Environment 17
4.2 Objectives for the TOE 17

5 Security Requirements 18

5.1 Conventions 18
5.2 Extended Components Definition 18
5.3 Functional Requirements 20
5.4 Assurance Requirements 37

6 TOE Summary Specification 38

6.1 Ethernet Encryption 38
6.2 Transmission Security 38
6.3 Certificate Management 39
6.4 Cryptographic Operations 39
6.5 Secure Administration 42
6.6 Trusted Path/Channels 43
6.7 Self-Protection 44
6.8 Audit 45

7 Rationale 46

7.1 Security Objectives Rationale 46
7.2 Security Requirements Rationale 47
7.3 TOE Summary Specification Rationale 53

List of Tables

Table 1: Evaluation identifiers 5
Table 2: Terminology 5
Table 3: TOE Interfaces 9
Table 4: TOE models and capabilities 12
Table 5: Threats 16
Table 6: Assumptions 16
Table 7: Security Objectives for the Operational Environment 17
Table 8: Security Objectives 17
Table 9: Extended Components 18
Table 10: Summary of SFRs 20
Table 11: Management of TSF Data 31
Table 12: Assurance Requirements 37
Table 13: Cryptographic Operations 39
Table 14: Algorithm Validation Certificates (CAVP) 41
Table 15: Security Objectives Mapping 46
Table 16: Suitability of Security Objectives 47
Table 17: Security Requirements Mapping 48
Table 18: Suitability of SFRs 50
Table 19: Map of SFRs to TSS Security Functions 53

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Senetas CN Series Ethernet Encryptors v5.5.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a high-speed, standards-based encryptor designed to secure voice, data and video information transmitted over Ethernet networks. The TOE also provide access control facilities using access rules for each defined Ethernet connection.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Senetas CN 4000/6000 Series Ethernet Encryptors v5.5.0 Build: 31224
Security Target	Senetas Distributed by Thales CN 4000/6000 Series Ethernet Encryptors v5.5.0 Security Target, v1.4

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) EAL2+ augmented (ALC_FLR.2)

1.4 Terminology

Table 2: Terminology

Term	Definition
Activation	Process of replacing default user credentials using RSA
CA	Certification Authority
CC	Common Criteria
CI	Connection Identifier (represents an established security association)
CLI	Command Line Interface
CM7	Senetas PC based remote Management Application
CRC	Cyclic Redundancy Check

Term	Definition
CSP	Critical Security Parameter
DEK	Data Encryption Key
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EtherType	A field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of the frame.
ETSI	European Telecommunications Standards Institute
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
KDK	Key Derivation Key
KEK	Key Encrypting Key
KID	Key ID
KMIP	Key Management Interoperability Protocol
KMS	Key Management Service
MAC	Media Access Control
NAE	Network-Attached Encryption – Safenet proprietary key management protocol.
NIST	National Institute of Standards and Technology
OAEP	Optimal Asymmetric Encryption Padding
OSP	Organisational Security Policy
QKD	Quantum Key Distribution – network distribution of QRA generated keys in accordance with defined standards (ETSI).

Term	Definition
QRA	Quantum Resistant Algorithms – Candidate algorithms supported by the Open Quantum Safe project.
RFC	Request for Comment
RSA	Rivest Shamir Adleman Public Key Algorithm
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	SSH File Transfer Protocol
SME	Secure Message Exchange
SMK	System Master Key
SNMPv3	Simple Network Management Protocol Version 3
SSH	Secure Shell
TACACS+	Terminal Access Control Access Control Server
TIM	Transport Independent Mode – Allows concurrent secure connections between encryptors over network layers 2, 3 and 4.
Traffic Analysis	The process of intercepting and examining messages in order to deduce information from patterns in communication.
TRANSEC	Transmission Security - used to disguise patterns in network traffic to prevent traffic analysis.
TSS	TOE Summary Specification
Tunnel	Equivalent to CI
VLAN	Virtual Local Area Network
X.509	Digital Certificate Standard

2 TOE Description

2.1 Type

4 The TOE is a network encryptor.

2.2 Usage

5 The CN Series Ethernet Encryptors are typically installed between an operator's private network equipment and public network connection and are used to secure data transiting over Ethernet networks. When operating at full bandwidth, the Ethernet Encryptor will not discard any valid Ethernet frame in all modes of operation.

6 Different user roles with different privileges are defined. The four defined roles are Administrator, Supervisor, Operator and Upgrader. Only the Administrator has unrestricted access to the security features of the encryptor and is able to install X.509 certificates that are required for the encryptor to start operation. The encryptors also provide an audit capability to support the effective management of the security features of the device. The audit capability records all management activities for security relevant events.

7 The TOE protects the confidentiality and, optionally, the integrity of transmitted data between secured sites (e.g. data centres) by cryptographic mechanisms. The TOE supports up to three AES modes: CTR, CFB and GCM (**Note:** see Table 4 for TOE models and supported AES modes).

The encryptors can be added to an existing network with complete transparency to the end user and network equipment.

8 An operational overview of the TOE can be found in Figure 1.

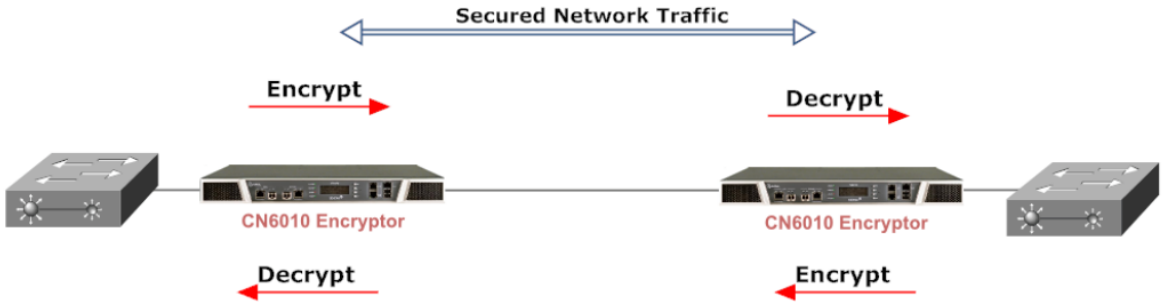

Figure 1: TOE operational overview

2.2.1 Physical Ports

9 Table 3 describes the TOE physical ports to further assist the reader in understanding how the TOE is used.

Table 3: TOE Interfaces

Physical Port	Use
Local port	The Local Port connects to the private network. See 'I/F' column in Table 4 for supported connectors / cable media.
Network port	The Network Port connects to the public network. See 'I/F' column in Table 4 for supported connectors / cable media.
Serial console	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 evaluated configuration. This port also allows administrative access and monitoring of operations. Username and password authentication is required to access this port.
Keypad	Allows entry of basic commands (**Note:** not available on all TOE models).
LCD and LEDs	The LCD displays basic configuration information in response to commands entered via the navigation keypad (**Note:** not available on all TOE models). The LEDs indicate basic TOE status information.
Management RJ-45 Ethernet port (LAN)	Supports management plane connections for SNMPv3, SSH, SFTP/FTPS, and Key Server over TLS.
USB	The USB port provides a mechanism for applying approved and properly signed firmware upgrades to the module.
Erase + Keypad	The concealed front panel "Emergency" Erase feature can be activated using a paperclip or similar tool and will immediately delete the System Master Key. The Erase feature functions irrespective of the powered state of the module.

2.2.2 Ethernet Processing

10 The TOE protects Ethernet frames by encrypting the payload of the frame. The twelve-byte Ethernet frame header is unchanged, which enables switching of the frame through an Ethernet network. The format of the Ethernet frame is shown in Figure 2.

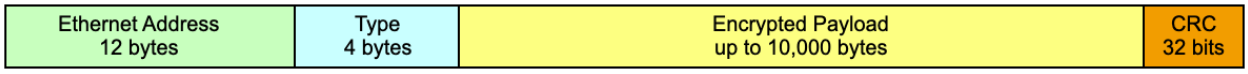

Figure 2: Ethernet Frame

11 Any combination of encrypted or unencrypted tunnels can be configured up to a maximum of 512 active connections for a standard Ethernet frame format. Each encrypted connection uses different encryption keys for each direction.

12 The TOE can be configured to operate in any one of the following Connection Modes:

a) **Point-to-Point (line) mode.** Supports a single encrypted CI/tunnel, and often used on dedicated links. In this mode, TRANSEC framing can be enabled to disguise patterns in traffic, thus preventing traffic analysis.

b) **MAC multipoint (mesh) mode.** Traffic between end points is encrypted based on the MAC address of the connected equipment.

c) **VLAN multipoint mode.** Traffic is encrypted based on VLAN IDs in the Ethernet header.

d) **Transport Independent Mode (TIM).** Traffic is encrypted based on Sender ID (SID) in the Senetas proprietary shim inserted in the Ethernet frame.

2.2.3 Key Management

13 Public key cryptography (RSA/ECDSA) and X.509 certificates are used to provide a fully automated key management system. The Key Encrypting Keys (KEKs) and the initial Data Encrypting Keys (DEKs) are securely transferred between encryptors using RSA-OAEP (in accordance with NIST SP 800-56B). Subsequent DEKs are transferred periodically between the encryptors encrypted using AES with the associated KEK and authenticated using HMAC-256.

14 Alternatively, ECDSA/ECDH uses ephemeral key agreement for the purpose of establishing DEKs in accordance with NIST SP800-56A.

2.2.3.1 System Master Key

15 A 256 bit System Master Key (SMK) is used with AES-CFB to protect private keys and passwords. The SMK is generated locally and stored in tamper protected memory. The SMK may optionally be a split key as described below.

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

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

2.2.3.2 Transport Independent Mode

18 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:

a) **Key Derivation Function (KDF).** Encryptors are securely loaded with the same Key Derivation Key (KDK) generated using the DRBG on an encryptor and distributed out-of-band via CM7. The KDK is used to derive the DEKs using a KDF that conforms to NIST SP 800-108 (counter mode using a Keyed HMAC).

b) **External Key Server using KMIP.** 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. DEKs are periodically updated using either a time-based mechanism or a frame counter based mechanism.

2.2.4 Control Plane

19 Figure 3 below depicts the control plane connections supported by the TOE. These are:

a) **Serial Console.** Local management via serial access to the CLI.

b) **SSH.** Remote management via SSH access to the CLI.

c) **SNMPv3.** Remote management via SNMPv3. The TOE administrator makes use of the CM7 application for this connection.

d) **File Server.** Remote file server used for firmware updates via SFTP (SSH) or FTPS (TLS).

e) **Key Server.** Remote KMIP or NAE service via TLS**.**

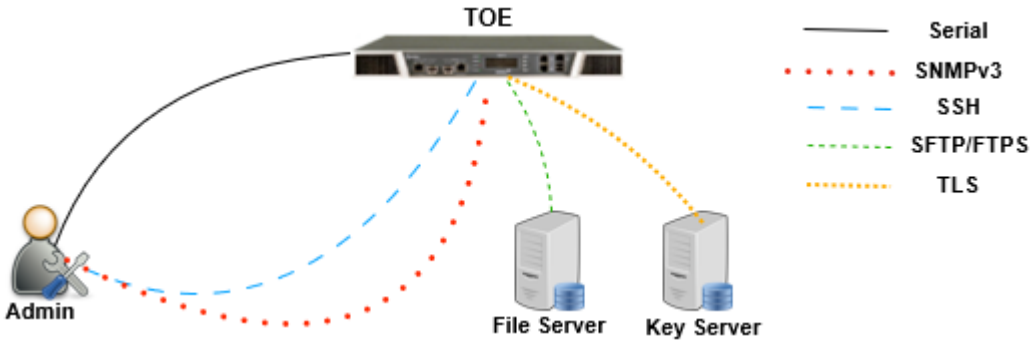

Figure 3: TOE Control Plane

2.3 Logical Scope

20 The logical scope of the TOE is comprised of the following security functions:

a) **Ethernet Encryption.** The TOE encrypts/decrypts Ethernet frames according to an administrator defined policy.

b) **Transmission Security**. The TOE supports TRANSEC to protect against traffic analysis in point-to-point (line) mode.

c) **Certificate Management**. The TOE supports X.509 CSR generation, X.509 certificate installation and management, and subsequent X.509 based authentication.

d) **Cryptographic Operations.** The TOE performs cryptographic operations in support of its security functions and provides management of all related keys.

e) **Secure Administration.** The TOE authenticates administrators and enforces role-based access control (RBAC). The TOE provides capabilities for local and remote management of its security functions.

f) **Trusted Path/Channels.** The TOE protects control plane communications via SSH, TLS, SFTP/FTPS and SNMPv3 as shown in Figure 3. The TOE protects the communication channel between encryptors (Ethernet Encryption).

g) **Self-Protection.** The TOE performs self-tests during start-up to verify code integrity and correction operation of its security functions. The TOE actively responds to tampering to protect key material.

h) **Audit.** The TOE maintains audit logs about the usage of its security functions.

2.3.1 Unevaluated Security Functions

21 The following security functions were not enabled or tested for the evaluation:

a) Remote authentication via TACACS+.

b) KeyVault – The TOE can sign certificates from credentials held within a key vault.

c) Hybrid Keys - The TOE supports the use of hybrid key establishment schemes combining NIST approved algorithms with candidate QKD/QRA systems. This functionality was not tested in the evaluated configuration.

d) Log Offloading – The TOE supports sending logs to a remote syslog server.

e) REST API – The TOE supports a RESTful HTTP(S) interface used for remote monitoring and issue detection.

2.4 Physical Scope

22 The physical boundary of the TOE is the encryptor hardware and firmware. Table 4 shows the TOE models. All TOE models use the same embedded software (version shown in Table 1) and share the same hardware architecture. Table 4 columns are as follows:

a) **Model.** The TOE model number.

b) **CPU & ASIC.** The CPU and ASIC for the TOE model.

c) **Hardware.** The part numbers associated with the hardware enclosure and supported power supply.

d) **Power.** Type of power supply for each hardware part number for a given model.

e) **Protocol / FPGA Bitstream.** The supported protocols and related FPGA bitstream, including whether TIM is supported.

f) **AES Modes.** The supported AES Modes.

g) **I/F.** The supported local/network port interfaces.

h) **LCD/Keypad.** Whether the model includes an LCD and Keypad.

Table 4: TOE models and capabilities

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
CN4010	ARM Cortex A9 Xilinx Zynq-7000	A4010B	DC (Plug Pack)	1G Ethernet	CFB, CTR, GCM	RJ45	No
				1G Ethernet TIM	CTR, GCM		
CN4020	ARM Cortex A9 Xilinx Zynq-7000	A4020B	DC (Plug Pack)	1G Ethernet	CFB, CTR, GCM	SFP	No
				1G Ethernet TIM	CTR, GCM		
CN6010	ARM Cortex A9	A6010B A6011B A6012B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet	CFB, CTR, GCM	RJ45 SFP	Yes

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
	Xilinx Zynq-7000			1G Ethernet TIM	CTR, GCM		
CN6110	ARM Cortex A9 Xilinx Zynq-7000	A6110B A6111B A6112B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet	CFB, CTR, GCM	RJ45 SFP+	Yes
				1G Ethernet TIM	CTR, GCM		
				10G Ethernet	CTR, GCM		
				10G Ethernet TIM	CTR, GCM		
CN6140	ARM Cortex A9 Xilinx Zynq-7000	A6140B A6141B A6142B	AC/AC Dual DC/DC Dual AC/DC Dual	1Gx1 Ethernet Single Port 1Gx4 Ethernet Multi Port	CFB, CTR, GCM	SFP+	Yes
				1Gx1 Ethernet TIM Single Port 1Gx4 Ethernet TIM Multi Port	CTR, GCM		
				10Gx1 Ethernet Single Port 10Gx2 Ethernet Multi Port	CTR, GCM		
				10Gx1 Ethernet TIM Single Port 10Gx4 Ethernet TIM Multi Port	CTR, GCM		
				10Gx4 Ethernet Multi Port	CTR		

23 The TOE models are shown in Figure 4 – 8 below.

Figure 4: CN4010 1G Ethernet Encryptor

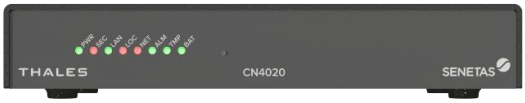

Figure 5: CN4020 1G Ethernet Encryptor

Figure 6: CN6010 1G Ethernet Encryptor

Figure 7: CN6110 1G Ethernet Encryptor

Figure 8: CN6140 1/10G Multi Port Ethernet Encryptor

2.4.1 Guidance Documents

24 The TOE includes the following guidance documents (PDF) which are made available via the Senetas customer portal:

a) Ethernet Encryptor CN4010 User Guide, (Windows™ / All Modes), Revision Date: January 2024

b) Ethernet Encryptor CN4020 User Guide, (Windows™ / All Modes), Revision Date: January 2024

c) Ethernet Encryptor CN6010 User Guide, (Windows™ / All Modes), Revision Date: January 2024

d) CN6110 Ethernet Encryptor User Guide, (Windows™ / All Modes), Revision Date: January 2024

e) Ethernet Encryptor CN6140 User Guide, (Windows™ / All Modes), Revision Date: January 2024

f) Senetas, Distributed by Thales, CN 4000/6000 Series Ethernet Encryptors v5.5.0 Preparative Procedures (AGD_PRE.1), v1.2

g) Senetas, Distributed by Thales, CN 4000/6000 Series Ethernet Encryptors v5.5.0 Operational User Guidance (AGD_OPE.1), v1.2

2.4.2 TOE Delivery

25 The encryptor device is delivered with the embedded software via commercial courier. The TOE embedded software may also be downloaded via the Senetas customer portal (https://support.senetas.com/).

26 The TOE User Guides are available to users with a maintenance contract via the Senetas customer portal. Users without a maintenance contract can access the FW and User Guides using a onetime temporal link on the Senetas SureDrop secure file sharing platform, provided by Senetas.

2.4.3 Non-TOE Components

27 The TOE operates with the following components in the environment:

a) **Remote RS232 terminal.** The TOE makes use of remote RS232 terminal to connect to the encryptor CLI via the management RS232 port.

b) **Remote SSH terminal.** The TOE makes use of SSH terminal to connect to the encryptor CLI via SSH.

c) **CM7 Application.** The TOE makes use of remote management software application and the terminal on which it is running.

d) **File Server**. The TOE can make use of file server for firmware upgrades.

e) **Key Server**. Remote KMIP or NAE service.

3 Security Problem Definition

3.1 Threats

Table 5: Threats

Identifier	Description
T.DATA_ACCESS	An attacker may modify and/or observe plaintext data being transmitted across a network link.
T.ADMIN_ATTACK	An attacker may observe management connections or impersonate an administrative user of the TOE which may compromise TSF data.
T.TRAFFIC_ANALYSIS	An attacker may perform traffic analysis of TOE protected network links to deduce confidential information.
T.ROGUE_DEVICE	An attacker may modify and/or observe TOE protected data by means of a counterfeit device.

3.2 Assumptions

Table 6: Assumptions

Identifier	Description
A.ADMIN	It is assumed that TOE administrators are competent to manage the TOE and can be trusted not to deliberately abuse their privileges.
A.PHYSICAL	It is assumed that the TOE is protected from unauthorized physical access.
A.NET_LOCATION	It is assumed that the TOE is appropriately located within the network to protect the desired network traffic.

3.3 Organizational Security Policies

28 None defined.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	Description
OE.PERSONNEL	TOE administrators shall be competent and can be trusted not to deliberately abuse his or her privileges to undermine security.
OE.PHYSICAL	The TOE shall be protected from unauthorized physical access.
OE.SETUP	The TOE shall be located appropriately within the network to protect the desired network traffic.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O.DATA_PROTECTION	The TOE shall protect the confidentiality and integrity of data transferred between TOE protected networks according to an administrator defined policy.
O.ADMIN_AUTH	The TOE shall prevent unauthorized access to administrative functions.
O.MGMT_PROTECT	The TOE shall protect the confidentiality and integrity of TOE management communications.
O.TRANSEC	The TOE shall provide the means to prevent Ethernet traffic analysis.
O.DEVICE_AUTH	The TOE shall prevent communication with unauthorized devices.
O.AUDIT	The TOE shall generate an audit trail of security relevant events.
O.SECURE_STATE	The TOE shall preserve a secure state in the event of a failure or tamper event occurring.

5 Security Requirements

5.1 Conventions

29 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

30 Table 9 identifies the extended components which are incorporated into this ST.

Table 9: Extended Components

Component	Title	Rationale
FDP_TSC_EXT.1	Transmission Security	No existing CC Part 2 SFRs address protection against traffic analysis. This family is added to the FDP class as transmission security is an aspect of user data protection.
FCS_SMC_EXT.1	Submask Combining	No existing CC Part 2 SFRs address submask combining. This extended component is based on the same SFR from the following evaluated and approved PPs: • collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition Version 2.0E • collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0E.

5.2.1 FDP_TSC_EXT Transmission Security

5.2.1.1 Family Behavior

31 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. Transmission security (TRANSEC) is used to disguise patterns in network traffic to prevent traffic analysis.

32 This family specifies the means by which transmission security is implemented to prevent traffic analysis.

5.2.1.2 Component Leveling

33 FDP_TSC_EXT.1, Transmission Security, requires the TSF to protect against traffic analysis.

5.2.1.3 Management: FDP_TSC_EXT.1

34 No specific management functions are identified.

5.2.1.4 Audit: FDP_TSC_EXT.1

35 There are no auditable events foreseen.

FDP_TSC_EXT.1 Transmission Security

Hierarchical to: No other components

Dependencies: None

FDP_TSC_EXT.1.1 The TSF shall disguise patterns in network traffic to prevent traffic analysis using the following technique(s): [assignment: types of TRANSEC techniques].

5.2.2 FCS_SMC_EXT Submask Combining

5.2.2.1 Family Behavior

36 This family specifies the means by which submasks (bitstrings) are combined to form cryptographic keys.

5.2.2.2 Component Leveling

37 FCS_SMC_EXT.1, Submask Combining, requires the TSF to combine the submasks in a predictable fashion.

5.2.2.3 Management: FCS_SMC_EXT.1

38 No specific management functions are identified.

5.2.2.4 Audit: FCS_SMC_EXT.1

39 There are no auditable events foreseen.

FCS_SMC_EXT.1 Submask Combining

Hierarchical to: No other components

Dependencies: [None, or FCS_COP.1 Cryptographic Operation]

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: XOR, SHA-256, SHA-384, SHA-512] to generate an [assignment: types of keys].

Application Note: FCS_COP.1 dependency is only required if SHA is selected.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCS_CKM.1/AES	Cryptographic key generation
FCS_CKM.1/RSA	Cryptographic key generation
FCS_CKM.1/ECDSA	Cryptographic key generation
FCS_CKM.2/RSA	Cryptographic key distribution
FCS_CKM.2/AES	Cryptographic key distribution
FCS_CKM.2/DH	Cryptographic key distribution
FCS_CKM.2/ECDH	Cryptographic key distribution
FCS_CKM.4/SMK	Cryptographic key destruction
FCS_CKM.4/PK	Cryptographic key destruction
FCS_CKM.4/AES	Cryptographic key destruction
FCS_COP.1/AES_Key	Cryptographic operation
FCS_COP.1/AES_Data	Cryptographic operation
FCS_COP.1/RSA_enc	Cryptographic operation
FCS_COP.1/SHA	Cryptographic operation
FCS_COP.1/HMAC	Cryptographic operation
FCS_COP.1/RSA_sign	Cryptographic operation
FCS_COP.1/ECDSA_sign	Cryptographic operation
FCS_SMC_EXT.1	Submask Combining
FDP_DAU.1	Basic Data Authentication
FDP_ITC.2	Import of user data with security attributes
FDP_IFC.1/ETH	Subset information flow control

Requirement	Title
FDP_IFF.1/ETH	Simple security attributes
FDP_IFC.1/KEY	Subset information flow control
FDP_IFF.1/KEY	Simple security attributes
FDP_TSC_EXT.1	Transmission Security
FDP_UCT.1	Basic data exchange confidentiality
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1/ETH	Inter-TSF trusted channel
FTP_ITC.1/CP	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *Device events (event log) and configuration changes (audit log).*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no additional details.*

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*users in the role of Administrator, Supervisor, Operator and Upgrader*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.2 Cryptographic support (FCS)

FCS_CKM.1/AES Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES* and specified cryptographic key sizes *128, 256 bits* that meet the following: *FIPS PUB 197 and NIST SP800-38A*.

FCS_CKM.1/RSA Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *2048 bits* that meet the following: *FIPS PUB 186-4*.

FCS_CKM.1/ECDSA Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ECDSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA* and specified cryptographic key sizes *P-256, P-384 and P-521* that meet the following: *FIPS PUB 186-4 Digital Signature Standard, Appendix B.*

FCS_CKM.2/RSA Cryptographic key distribution

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1/RSA	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *RSA-OAEP public key* that meets the following: *NIST SP800-56B*.

FCS_CKM.2/AES Cryptographic key distribution

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1/AES	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *AES-256 CFB using HMAC-256 for authentication* that meets the following: *FIPS PUB 197, NIST SP800-38A and FIPS PUB 198-1.*

FCS_CKM.2/DH Cryptographic key distribution

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1/DH	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *Diffie-Hellman key agreement* that meets the following: *PKCS#3*.

FCS_CKM.2/ECDH Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1/ECDH The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *Elliptic Curve Diffie-Hellman* that meets the following: *NIST SP800-56A*.

FCS_CKM.4/SMK Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/SMK The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *none*.

FCS_CKM.4/PK Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/PK The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *deletion of the files containing these keys (RSA and ECDSA keys)* that meets the following: *none*.

FCS_CKM.4/AES Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *disconnection of power supply* that meets the following: *none*.

Application Note: All KEKs and DEKs used to encrypt the payload of the Ethernet frame are held in volatile memory. Loss of electrical power will destroy all KEKs/DEKs.

FCS_COP.1/AES_Key Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/AES_Key The TSF shall perform *encryption/decryption using the D.MASTER_KEY on the encryptor private RSA and ECDSA keys and user passwords* in accordance with a specified cryptographic algorithm *AES Cipher Feedback (CFB)* and cryptographic key sizes *256 bits* that meet the following: *FIPS PUB 197 and NIST SP800-38A*.

FCS_COP.1/AES_Data Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/AES_Data The TSF shall perform *data encryption/decryption* in accordance with a specified cryptographic algorithm *AES on self-synchronising Cipher Feedback (CFB), counter (CTR) and Galois counter (GCM) modes* and cryptographic key sizes *128 and 256 bits* that meet the following: *FIPS PUB 197, and NIST SP800-38A (CFP & CTR) or NIST SP800-38D (GCM)*.

FCS_COP.1/RSA_enc Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/RSA_enc The TSF shall perform *public key encryption* in accordance with a specified cryptographic algorithm *RSA-OAEP* and cryptographic key sizes *2048 bits* that meet the following: *NIST SP800-56B*.

FCS_COP.1/SHA Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/SHA The TSF shall perform *message digest generation/verification* in accordance with a specified cryptographic algorithm *SHA-256, SHA-384, SHA-512* and cryptographic key sizes *256, 384, 512 bits* that meet the following: *FIPS PUB 180-4*.

FCS_COP.1/HMAC Cryptographic Operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/HMAC The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512* and cryptographic key sizes *160, 256, 384, 512 bits* and message digest sizes *160, 256, 384, 512* bits that meet the following: *FIPS PUB 198-1*.

FCS_COP.1/RSA_sign Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/RSA_sign The TSF shall perform *digital signature generation/verification* in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *2048 bits* that meet the following: *PKCS#1*.

FCS_COP.1/ECDSA_sign Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1/ECDSA_sign The TSF shall perform *digital signature generation/verification* in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *P-256, P-384 or P-521* that meet the following: *FIPS PUB 186-4*.

FCS_SMC_EXT.1 Submask Combining

Hierarchical to: No other components

Dependencies: [None, or FCS_COP.1 Cryptographic Operation]

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [XOR] to generate an [*Split SMK*].

5.3.3 User Data protection (FDP)

FDP_DAU.1 Basic Data Authentication

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of the *activation Certificate from an encryptor and activation data generated by CM7 for an encryptor*.

FDP_DAU.1.2 The TSF shall provide *administrators* with the ability to verify evidence of the validity of the indicated information.

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_ITC.2.1 The TSF shall enforce the *Import SFP* when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *no additional rules*.

Application Note: This SFR fulfills FCS_COP dependencies when keys or submask are imported from a Key Server.

FDP_IFC.1/ETH Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/ETH The TSF shall enforce the *Information Flow Control SFP* on
Subjects: S.Host
Objects: Ethernet frames
Operation: Encrypt, bypass or discard.

FDP_IFF.1/ETH Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/ETH The TSF shall enforce the *Ethernet SFP* based on the following types of subject and information security attributes:

- *MAC address contained in the Ethernet frame header in MAC mode*
- *VLAN ID contained in the Ethernet frame header in VLAN mode*
- *SID contained within the Senetas proprietary shim in the Ethernet frame when TIM is enabled*

FDP_IFF.1.2/ETH The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *The MAC address or VLAN ID in the Ethernet header or SID in the shim is listed in the CI, then the defined operation in the CI is allowed.*

FDP_IFF.1.3/ETH The TSF shall enforce the *additional Ethernet SFP rules*:

- *If the operation in the CI is defined as "encrypt" then the Ethernet frame will be passed with the Ethernet payload encrypted/decrypted.*
- *If the operation in the CI is defined as "bypass" then the Ethernet frame will be passed without modification.*
- *If the operation in the CI is defined as "discard" then the Ethernet frame will be discarded without further action.*

FDP_IFF.1.4/ETH The TSF shall explicitly authorize an information flow based on the following rules: *in point-to-point mode all frames shall be processed according to FDP_IFF.1.3*.

FDP_IFF.1.5/ETH The TSF shall explicitly deny an information flow based on the following rules: *none*.

FDP_IFC.1/KEY Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/KEY The TSF shall enforce the *Import SFP* on
Subjects: S.Host, S.KeyServer
Objects: Externally Generated Keys and Submasks
Operation: Import

FDP_IFF.1/KEY Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/KEY The TSF shall enforce the *Import SFP* based on the following types of subject and information security attributes:

- *KMIP attributes*
- *NAE attributes*

FDP_IFF.1.2/KEY The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *Externally generated keys and submasks may be imported from S.KeyServer if requested by the TOE (S.Host) according to the KMIP or NAE protocols.*

FDP_IFF.1.3/KEY The TSF shall enforce the *additional Import SFP rules*: *S.Host shall authenticate the identity of S.KeyServer according to the KMIP or NAE protocols.*

FDP_IFF.1.4/KEY The TSF shall explicitly authorize an information flow based on the following rules: *none*.

FDP_IFF.1.5/KEY The TSF shall explicitly deny an information flow based on the following rules: *none*.

FDP_TSC_EXT.1 Transmission Security

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions
FCS_CKM.1 Cryptographic Key Generation
FCS_CKM.2 Cryptographic Key Distribution
FCS_COP.1 Cryptographic Operation

FDP_TSC_EXT.1.1 The TSF shall disguise patterns in network traffic to prevent traffic analysis using the following technique(s): *fixed Ethernet frame size and transmission rate*.

Application Note: Transmission Security (or TRANSEC) can only be enabled when the TOE is configured to operate in the point-to-point (line) connection mode.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the *Ethernet SFP* to transmit and receive user data in a manner protected from unauthorised disclosure.

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *three (3)* unsuccessful authentication attempts occur related to *the last successful authentication of a user using the console port*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall *disable the user account for three minutes*.

FIA_UAU.2 User authentication before any action

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.5 Security Management (FMT)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the *Ethernet SFP* to restrict the ability to change_default, modify the security attributes *MAC address, VLAN ID or SID for Ethernet information flows* to *U.Administrator and U.Supervisor*.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.3.1 The TSF shall enforce the *Ethernet SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *U.Administrator or U.Supervisor* to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *Create, Query, Modify, Delete as shown in Table 11*] **on** the [*TSF data shown in Table 11*] to [*the roles shown in Table 11*].

Table 11: Management of TSF Data

Admin	Supv	Oper	Upgr	Management Function	TSF Data	Operation
✓	✓			Set Real Time Clock	Datetime	Q, M
✓				Load Module Certificate	RSA or ECDSA Public and Private Keys	C, M

Admin	Supv	Oper	Upgr	Management Function	TSF Data	Operation
✓				Create / Modify / Delete User Account	Username Privilege level Status (Active, Disabled) Console Access SNMP Access Password	C, Q, M, D
✓	✓	✓	✓	View User Account	Username Privilege level Status (Active, Disabled) Console Access SNMP Access	Q
✓	✓			Edit Connection Action Table (Bypass)	Connection Action Table	Q, M
✓	✓	✓	✓	View Connection Action Table	Connection Action Table	Q
✓	✓	✓	✓	Show Firmware Version	Firmware version	Q
✓				Clear Audit Trail	Audit Log	D
✓	✓	✓	✓	View Audit Trail	Audit Log	Q
✓				Clear Event Log	Event Log	D
✓	✓	✓	✓	View Event Log	Event Log	Q
✓	✓	✓	✓	View FIPS Mode Status	FIPS Mode Status	Q
✓				Change FIPS Mode Status	FIPS Mode Status	M
✓	✓			Run Self Test (Reboot Command)	None	n/a
✓			✓	Install Firmware Upgrade	None	n/a

Admin	Supv	Oper	Upgr	Management Function	TSF Data	Operation
✓			✓	Establish FTPS (TLS) Session	None	n/a
✓			✓	Establish SFTP (SSH) Session	None	n/a
✓	✓			Re/Start Secure Connection	None	n/a
✓				Generate X.509v3 Certificate Signing Request	RSA Private Key and RSA Public Key or ECDSA Private Key and ECDH Public Key	C
✓				Erase Module – Zeroize (Console Command)	System Master Key and all CSP data stored in non-volatile memory	D
✓	✓	✓	✓	Establish a Remote SNMP Session	None	n/a
✓	✓	✓	✓	Establish a Remote CLI Session	None	n/a
✓				Configure All Other Encryptor Settings	TSF Configuration	Q,M

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) Management Functions specified in Table 11*.*

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles *Administrator, Supervisor, Operator and Upgrader*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *self-tests return a fail result.*

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *attempts, by opening the unit, to gain physical access* to the *key material* by responding automatically such that the SFRs are always enforced.

Application Note: If the case is opened, then the system master key (SMK) used to encrypt the RSA/ECDSA private keys and user passwords is automatically erased.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of *the TSF*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *stored TSF executable code.*

5.3.7 TOE access (FTA)

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a *period of 10 minutes.*

Application Note: Applies to CLI (local and remote).

5.3.8 FTP (Trusted Path/Channels)

FTP_ITC.1/ETH Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/ETH The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure*.*

FTP_ITC.1.2/ETH The TSF shall permit the TSF and another trusted IT product to initiate communication via the trusted channel*.*

FTP_ITC.1.3/ETH The TSF shall initiate communication via the trusted channel for *all Ethernet frames as defined by the Ethernet SFP.*

FTP_ITC.1/CP Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/CP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure*.*

FTP_ITC.1.2/CP The TSF shall permit *the TSF* to initiate communication via the trusted channel*.*

FTP_ITC.1.3/CP The TSF shall initiate communication via the trusted channel for*:*

- *Key Servers via TLS*
- *File Servers via SFTP (SSH) or FTPS (TLS)*

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for:

- *Remote management via SSH*
- *Remote management via SNMPv3*

5.4 Assurance Requirements

40 The TOE security assurance requirements are summarized in Table 12 commensurate with EAL2+ (ALC_FLR.2).

Table 12: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Ethernet Encryption

Related SFRs: FDP_IFC.1/ETH, FDP_IFF.1/ETH, FTP_ITC.1/ETH, FDP_UCT.1, FMT_MSA.3

41 The TOE uses X.509v3 certificates to establish an authenticated communications channel between itself and other Encryptors. Both encryptors must have a valid X.509 certificate, in which the root trust anchor can be validated (trusted CA).

42 The TOE controls the flow of Ethernet frames received on the private and public network interfaces as follows:

a) **Point-to-Point (line) mode.** Supports a single encrypted CI/tunnel, and often used on dedicated links.

b) **MAC multipoint (mesh) mode.** Traffic between end points is encrypted based on the MAC address of the connected equipment.

c) **VLAN multipoint mode.** Traffic is encrypted based on VLAN IDs in the Ethernet header.

d) **Transport Independent Mode (TIM).** Traffic is encrypted based on Sender ID (SID) in the Senetas proprietary shim inserted in the Ethernet frame.

43 The TOE determines the appropriate action to take on any given frame by examining the list of entries in the CI table. The TOE will either encrypt/decrypt, discard or bypass (pass unchanged) the frame. By default, for a given address that is not listed in the CI table the frame is discarded.

44 If encryption is required, the encryptor performs hardware-based AES encryption on the Ethernet frame payload and a configurable portion of the header (see Cryptographic Operations below for further details).

45 The CI table initially contains no entries and hence all frames are discarded. The Administrator and Supervisor roles can specify alternative values in the CI table to override the default values.

6.2 Transmission Security

Related SFRs: FCS_COP.1/AES_Data, FDP_TSC_EXT.1, FMT_SMF.1

46 In point-to-point (line) mode, the TOE can be configured to implement TRANSEC, in which case the TOE generates and transmits fixed-size encrypted Ethernet frames at a constant frame rate on the public network interface.

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

48 In the absence of user data from the private network interface the TOE fills the transmitted frames with pseudo-random or encrypted data such that it cannot be distinguished from encrypted user data.

49 The TOE may (under policy) bypass certain control plane Ethernet Operations, Administration and Management frames that are necessary for correct operation of the network.

50 The transmitted encrypted Ethernet frame rate and size are both configurable.

51 Ethernet headers of encrypted traffic (including both the source and destination MAC addresses and other optional header fields (VLAN tag, MPLS shim, etc.) are also configurable.

6.3 Certificate Management

Related SFRs: FCS_COP.1/RSA_sign, FCS_COP.1/ECDSA_sign, FDP_DAU.1, FMT_MTD.1

52 Each encryptor must have one or more X.509v3 certificates installed before the operation of the encryptor can start. Before X.509v3 certificates can be installed, each encryptor must have the default user account credentials updated. This process is referred to as activation and is performed via CM7 (i.e. the management application).

53 When activating an encryptor, CM7 requests a new public key from the encryptor which is sent contained within a Senetas proprietary V2 certificate. The encryptor hashes the certificate using SHA-256 to create a validation code. The validation code is displayed on the front panel of the encryptor or on the CLI (where no front panel display exists). CM7 also hashes the received data and displays the validation code. Both the CM7 user and the remote operator must agree that the validation codes are the same before the CM7 encrypts the new user credentials.

54 When CM7 returns the encrypted credentials back to the encryptor, the same process is repeated again with the CM7 user and the remote operator agreeing that the validation codes are the same before the default user account is updated by the encryptor. Alternatively a user can locally activate an encryptor via the CLI on the console port using the “activate –l” command to replace the unit’s default administrator credentials.

55 Once activated, the TOE can generate Certificate Signing Requests (CSRs) for signing by an external CA. The TOE supports subsequent loading of X.509v3 certificates.

6.4 Cryptographic Operations

Related SFRs: FCS_CKM.1/AES, FCS_CKM.1/RSA, FCS_CKM.1/ECDSA, FCS_CKM.2/RSA, FCS_CKM.2/DH, FCS_CKM.2/ECDH, FCS_CKM.4/SMK, FCS_CKM.4/PK, FCS_CKM.4/AES, FCS_COP.1/AES_Key, FCS_COP.1/AES_Data, FCS_COP.1/RSA_enc, FCS_COP.1/SHA, FCS_COP.1/HMAC, FCS_COP.1/RSA_sign, FCS_COP.1/ECDSA_sign, FCS_SMC_EXT.1, FDP_ITC.2, FDP_IFC.1/KEY, FDP_IFF.1/KEY

56 The TOE performs cryptographic operations in support of its security functions and provides management of all related keys. Key management capabilities are described at section 2.2.3.

57 Table 13 identifies the cryptographic operations and related security functions supported by the TOE. Related standards are identified in section 5.3.2.

Table 13: Cryptographic Operations

SFR	Details	Security Function / Usage
FCS_CKM.1/AES	Generation of 128-bit and 256-bit symmetric keys.	Ethernet Encryption (KEKs, DEKs) Trusted Path/Channels – TLS, SSH, SNMPv3 System Master Key (SMK)
FCS_CKM.1/RSA	Generation of 2048-bit RSA keys	Certificate Management Ethernet Encryption – authentication

SFR	Details	Security Function / Usage
FCS_CKM.1/ECDSA	Generation of ECDSA P-256, P-384 or P-521 curves	Certificate Management Ethernet Encryption – authentication Trusted Path/Channels – SSH, TLS
FCS_CKM.2/RSA	RSA-OAEP key distribution	Ethernet Encryption – key distribution
FCS_CKM.2/AES	AES-256 CFB using HMAC-256 for authentication	Ethernet Encryption – key distribution
FCS_CKM.2/DH	PKCS#3 Diffie-Hellman key agreement	SNMPv3 shared secret
FCS_CKM.2/ECDH	ECDH ephemeral key agreement	Ethernet Encryption – key distribution Trusted Path/Channels – TLS
FCS_CKM.4/SMK	Zeroization of the SMK. If the case is opened, then the SMK used to encrypt the RSA/ECDSA private keys and user passwords is automatically erased.	Self-Protection
FCS_CKM.4/PK	RSA and ECDSA encrypted keys – file deletion.	Cryptographic Operations – key destruction
FCS_CKM.4/AES	Loss of electrical power will destroy all AES KEKs/DEKs in volatile memory.	Cryptographic Operations – key destruction
FCS_COP.1/AES_Key	AES-256-CFB encryption/decryption of RSA and ECDSA keys and user passwords	Cryptographic Operations – CSP protection
FCS_COP.1/AES_Data	AES-128/256-CFB/CTR/GCM encryption/decryption of data	Ethernet Encryption – Ethernet payload encryption Trusted Patch/Channels – TLS, SSH, SNMPv3 data encryption
FCS_COP.1/RSA_enc	2048-bit RSA encryption (RSA-OAEP)	Ethernet Encryption – key distribution

SFR	Details	Security Function / Usage
FCS_COP.1/SHA	SHA-1, SHA-256, SHA-384, SHA-512	Certificate Management – for activation, the encryptor hashes the certificate using SHA-256 to create a validation code Ethernet Encryption – X.509v3 certificates use SHA-256 Trusted Path/Channels – TLS, SSH, SNMPv3
FCS_COP.1/HMAC	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Trusted Path/Channels – TLS, SSH, SNMPv3
FCS_COP.1/RSA_sign	RSA digital signature generation/verification	Certificate Management Ethernet Encryption – authentication
FCS_COP.1/ ECDSA_sign	ECDSA digital signature generation/verification	Certificate Management Ethernet Encryption – authentication Trusted Path/Channels – SSH, TLS
FCS_SMC_EXT.1	XOR	Cryptographic Operations – key combining for SMK split key (2.2.3.1).

Table 14: Algorithm Validation Certificates (CAVP)

Library	Description	Certificate
CN Series Common Crypto Library	Provides all software based cryptographic services.	A3451
CN4010 Crypto Module	Cryptographic Accelerator (AES Ethernet)	A3435
	Cryptographic Accelerator (AES TIM)	A3436
CN4020 Crypto Module	Cryptographic Accelerator (AES Ethernet)	A3437
	Cryptographic Accelerator (AES TIM)	A3438
CN6010 Crypto Module	Cryptographic Accelerator (AES Ethernet)	A3439
	Cryptographic Accelerator (AES TIM)	A3440

Library	Description	Certificate
CN6110 Crypto Module	Cryptographic Accelerator 1GbE (AES Ethernet)	A3549
	Cryptographic Accelerator 1GbE (AES TIM)	A3443
	Cryptographic Accelerator 10GbE (AES Ethernet)	A3441
	Cryptographic Accelerator 10GbE (AES TIM)	A3442
CN6140 Crypto Module	Cryptographic Accelerator 1GbE (AES Ethernet)	A3445
	Cryptographic Accelerator 1GbE (AES TIM)	A3460
	Cryptographic Accelerator 10GbE (AES Ethernet)	A3448
	Cryptographic Accelerator 10GbE (AES TIM)	A3444
	Cryptographic Accelerator 4x10GbE (AES Ethernet)	A3492

6.5 Secure Administration

Related SFRs: FIA_AFL.1, FIA_UAU.2, FIA_UID.2, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3

58 To modify and view any of the security attributes of the TOE, authorised users must identify and authenticate via one of two mechanisms depending on whether they are using the SNMPv3 functionality or the console management functionality. Identification and Authentication services are only performed by the encryptor.

59 For local (CLI) management using the local console port of the encryptor, users logon by supplying a user ID and their authentication password. The encryptor then compares the user ID and the password supplied with the local authentication password. If the authentication password does not match for that user ID in the encryptor User Account Table, then identification and authentication fails, the console session is not started. After three consecutive unsuccessful logon attempts, the console will be disabled for three minutes. If the user ID and authentication password match the entry in the user table, a console session is opened.

60 Alternatively the CLI can be accessed remotely via SSH. When configuring remote CLI access, the authentication algorithm is restricted to ECDSA. ECDSA is restricted to NIST P-256, P-384 and P-521 curves.

61 For remote management using SNMPv3, the CM7 remote management station will generate an appropriate authentication key, used to authenticate the remote management data, and a privacy key used to encrypt the remote management data. Both keys are generated on CM7 after retrieving the SNMPv3 Engine ID of the encryptor and via the generation of shared secret via a Diffie-Hellman Key-Agreement. The remote management data is associated with a user ID entered by the user on CM7 to make the SNMPv3 packet. The authenticated SNMPv3 packets are then sent to the encryptor. The User ID and local authentication passwords are stored within the User Account Table of the encryptor, with the first administrator account being created during the initialisation of the encryptor. The encryptor can encrypt SNMPv3 packets using 128-bit AES with keys derived from the engine ID of the encryptor and the user's privacy key. If the encryptor cannot decrypt the data, or the authentication process as specified in RFC2574 fails,

then the identification and authentication of that SNMPv3 data fails, the SNMPv3 data is discarded. Each SNMPv3 packet received is identified and authenticated in this way.

62 The console user session will be automatically terminated by the encryptor after a period of 10 minutes as a result of user inactivity.

63 The TOE defines four roles for accessing the TSFs:

a) Administrators: can change defaults, query, modify, delete and clear the CI entries and User accounts, perform activation and install X.509 certificates, clear the audit log, view the audit log, set the system time and remotely upgrade the firmware via SFTP or FTPS.

b) Supervisors: can change defaults, query, modify, delete and clear the CI entries, view the User accounts table and audit log and set the system time.

c) Operators: can query the CI and User Account tables only, and view the audit log.

d) Upgraders: can remotely upgrade the firmware via either USB, SFTP or FTPS, query the CI and User Account tables and view the audit log.

64 When the TOE is accessed, the TOE associates users with these roles and prevents a user from performing operations on the TSFs that they are not authorised to perform.

65 The User Table initially has one default administrator account. By default, all other users are created as operators unless the administrator overrides this value.

66 Firmware update image is signed, and the TOE checks its authenticity and integrity before performing firmware upgrade.

6.6 Trusted Path/Channels

Related SFRs: FTP_ITC.1/CP, FTP_TRP.1

67 The TOE protects control plane communications via SSH, TLS, SFTP/FTPS and SNMPv3 as shown in Figure 3.

6.6.1 SNMPv3

68 Diffie-Hellman Key Agreement (Group 14) is employed to establish secure 128 bit AES (CFB) 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 using HMAC-SHA1. Data Origin Authentication, based on the names and passwords, ensures the authenticity of the user claiming to have sent the command.

6.6.2 SSH & SFTP

69 The TOE supports SSHv2 for firmware upgrade image transfer via SFTP (the encryptor is the SSH client) and remote access to the CLI (the encryptor is the SSH server).

70 The TOE's implementation of SSHv2 has the following characteristics:

a) Authentication: ECDSA (NIST P-256, P-384 and P-521)

b) Key Exchange: ECDH (NIST P-256, P-384 and P-521), DH (minimum DH key size allowed is 2048 bits)

c) Encryption: AES-256-CTR, AES-128-CTR

d) Data Integrity: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512

71 The TOE SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key.

6.6.3 TLS & FTPS

72 The TOE implements a TLS v1.2 client for firmware upgrade via FTPS, and communication with remote key servers. The TOE's TLS v1.2 implementation supports the following cipher suites:

a) TLS_ECDHE_ECDSA_WITH_AES_256_CBC-SHA384

b) TLS_ECDHE_ECDSA_WITH_AES_128_CBC-SHA256

c) TLS_ECDHE_ECDSA_WITH_AES_256_GCM-SHA384

d) TLS_ECDHE_ECDSA_WITH_AES_128_GCM-SHA256

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

6.7 Self-Protection

Related SFRs: FPT_FLS.1, FPT_PHP.3, FPT_TST.1

6.7.1 Self-Tests

74 The encryptor performs self-tests during start-up to check that the underlying functionality of the TSF is functioning correctly. The tests include verification of the cryptographic processors, Random Noise Source, Firmware integrity and Software integrity. The results of the self-tests are audited. If any of the self-tests fail, then the TOE will preserve a secure state and all output is suppressed.

6.7.2 Tamper Protection

75 Zeroization will be initiated immediately upon detection of a tamper event (opening of the TOE enclosure). The Tamper Circuit is active at all times. The tamper initiated zeroization process achieves the following:

a) 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.

b) When powered on and the Tamper Circuit is triggered, the module will automatically:

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

   ii) Log the tamper event to the Audit Log,

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

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

   v) REBOOT the module.

c) 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:

   i) Log the tamper event to the Audit log,

ii) Initiate the Zeroization sequence,

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

d) When the BOOT sequence has completed the module will have:

i) Generated a new System Master Key,

ii) Re-created the default administration account,

iii) Set the encryption mode to DISCARD,

iv) Entered the factory default state ready for Configuration

6.8 Audit

Related SFRs: FAU_GEN.1, FAU_SAR.1, FPT_STM.1

76 Audit data is generated only within the encryptor, and stored in an audit table in non-volatile memory. All auditable events are associated with operations that occur in the encryptor. The encryptor is able to generate an audit record for each of the auditable events.

77 The TOE generates the following audit events:

a) Device events per Appendix A-2 Event Log Messages of the TOE User Guide

b) Configuration changes per Appendix A1 Audit Log Messages of the TOE User Guide

78 The TOE contains a Real Time Clock (RTC) from which a timestamp is obtained for each audit record.

79 Authorised users can view the audit log, using SNMPv3 remote management from CM7 or via the CLI. In each case, the user is identified and authenticated before access is granted to the audit log. In each case, the data is presented in a human readable format, with CM7 and the console presenting the data as a scrolled list of audit records.

80 The audit log has a finite size for logging audit records. Once this space has been used, the audit log is either cycled back around, or disabled as selected by the Administrator. The Administrator is also permitted to clear the audit log at any time.

7 Rationale

7.1 Security Objectives Rationale

81 Table 15 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 15: Security Objectives Mapping

	T.DATA_ACCESS	T.ADMIN_ATTACK	T.TRAFFIC_ANALYSIS	T.ROGUE_DEVICE	A.ADMIN	A.PHYSICAL	A.NET_LOCATION
O.DATA_PROTECTION	X						
O.ADMIN_AUTH		X					
O.MGMT_PROTECT		X					
O.TRANSEC			X				
O.DEVICE_AUTH				X			
O.AUDIT		X					
O.SECURE_STATE	X						
OE.PERSONNEL					X		
OE.PHYSICAL						X	
OE.SETUP							X

82 Table 16 provides the justification to show that the security objectives are suitable to address the security problem.

Table 16: Suitability of Security Objectives

Element	Rationale
T.DATA_ACCESS	O.DATA_PROTECTION counters this threat by requiring that the TOE protect the confidentiality and integrity of data transferred between TOE protected networks. O.SECURE_STATE supports mitigation of this threat by ensuring that the TOE maintains a secure state in the event of a failure or tamper event.
T.ADMIN_ATTACK	O.ADMIN_AUTH counters this threat by requiring that the TOE prevent unauthorized use of administrative functions. O.MGMT_PROTECT further mitigates this threat by requiring that the TOE protect the confidentiality and integrity of TOE management communications. O.AUDIT counters this threat by ensuring all security relevant events are recorded and the audit trail can be reviewed.
T.TRAFFIC_ANALYSIS	O.TRANSEC counters this threat by requiring the TOE to provide the means to prevent Ethernet traffic analysis.
T.ROGUE_DEVICE	O.DEVICE_AUTH counters this threat by requiring the TOE to prevent communication with unauthorized devices.
A.ADMIN	OE.PERSONNEL upholds the assumption by restating the assumption as an objective for the TOE environment.
A.PHYSICAL	OE.PHYSICAL upholds the assumption by restating the assumption as an objective for the TOE environment.
A.NET_LOCATION	OE.SETUP upholds the assumption by restating the assumption as an objective for the TOE environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

83 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 17: Security Requirements Mapping

	O.DATA_PROTECTION	O.ADMIN_AUTH	O.MGMT_PROTECT	O.TRANSEC	O.DEVICE_AUTH	O.AUDIT	O.SECURE_STATE
FAU_GEN.1						X	
FAU_SAR.1						X	
FCS_CKM.1/AES	X		X				
FCS_CKM.1/RSA	X				X		
FCS_CKM.1/ECDSA	X		X		X		
FCS_CKM.2/RSA	X						
FCS_CKM.2/AES	X						
FCS_CKM.2/DH			X				
FCS_CKM.2/ECDH	X		X				
FCS_CKM.4/SMK							X
FCS_CKM.4/PK	X		X				X
FCS_CKM.4/AES	X		X				X
FCS_COP.1/AES_Key							X
FCS_COP.1/AES_Data	X		X				
FCS_COP.1/RSA_enc	X						
FCS_COP.1/SHA	X		X		X		
FCS_COP.1/HMAC			X				
FCS_COP.1/RSA_sign	X				X		

	O.DATA_PROTECTION	O.ADMIN_AUTH	O.MGMT_PROTECT	O.TRANSEC	O.DEVICE_AUTH	O.AUDIT	O.SECURE_STATE
FCS_COP.1/ECDSA_sign	X		X		X		
FCS_SMC_EXT.1	X						X
FDP_DAU.1					X		
FDP_ITC.2	X						
FDP_IFC.1/ETH	X						
FDP_IFF.1/ETH	X						
FDP_IFC.1/KEY	X						
FDP_IFF.1/KEY	X						
FDP_TSC_EXT.1				X			
FDP_UCT.1	X						
FIA_AFL.1		X					
FIA_UAU.2		X					
FIA_UID.2		X					
FMT_MSA.1	X						
FMT_MSA.3	X						
FMT_MTD.1		X					
FMT_SMF.1	X	X	X	X	X	X	X
FMT_SMR.1		X					
FPT_FLS.1							X
FPT_PHP.3							X

	O.DATA_PROTECTION	O.ADMIN_AUTH	O.MGMT_PROTECT	O.TRANSEC	O.DEVICE_AUTH	O.AUDIT	O.SECURE_STATE
FPT_STM.1						X	
FPT_TST.1							X
FTA_SSL.3		X					
FTP_ITC.1/ETH	X				X		
FTP_ITC.1/CP			X				
FTP_TRP.1			X				

Table 18: Suitability of SFRs

Objectives	SFRs
O.DATA_PROTECTION	**FCS_CKM.1/AES** specifies generation of AES keys which are used for Ethernet encryption. **FCS_CKM.1/RSA** specifies generation of RSA keys for Ethernet encryption authentication. **FCS_CKM.1/ECDSA** specifies generation of ECDSA keys for Ethernet encryption authentication. **FCS_CKM.2/RSA** specifies RSA asymmetric key distribution for Ethernet encryption. **FCS_CKM.2/AES** specifies AES key distribution for Ethernet encryption. **FCS_CKM.2/ECDH** specifies EC asymmetric key distribution for Ethernet encryption. **FCS_CKM.4/PK** requires destruction of private keys used for Ethernet encryption. **FCS_CKM.4/AES** requires destruction of symmetric keys used for Ethernet encryption. **FCS_COP.1/AES_Data** specifies AES encryption used for payload encryption.

Objectives	SFRs
	FCS_COP.1/RSA_enc specifies RSA encryption used in key distribution. **FCS_COP.1/SHA** specifies SHA which is used in digital signatures supporting Ethernet encryption. **FCS_COP.1/RSA_sign** specifies RSA digital signatures supporting Ethernet encryption. **FCS_COP.1/ECDSA_sign** specifies ECDSA digital signatures supporting Ethernet encryption. **FCS_SMC_EXT.1** specifies XOR submask combing used in hybrid key establishment supporting Ethernet encryption. **FDP_ITC.2** requires controlled import of keys when using external key servers supporting Ethernet encryption. **FDP_IFC.1/ETH** specifies attributes for Ethernet encryption policy. **FDP_IFF.1/ETH** specifies rules for Ethernet encryption policy. **FDP_IFC.1/KEY** specifies attributes for import of keys. **FDP_IFF.1/KEY** specifies rules for import of keys when using external key servers supporting Ethernet encryption. **FDP_UCT.1** requires enforcement of Ethernet encryption policy. **FMT_MSA.1** requires restricted management of Ethernet encryption policy attributes. **FMT_MSA.3** requires restrictive default values for Ethernet encryption policy attributes. **FMT_SMF.1** requires the capability to manage Ethernet encryption policy attributes. **FTP_ITC.1/ETH** requires a trusted channel between encryptors.
O.ADMIN_AUTH	**FIA_AFL.1** requires limiting the number of unsuccessful authentication attempts before imposing a timeout on that user account. **FIA_UAU.2 and FIA_UID.2** provide the capability for identifying and authenticating users. **FMT_MTD.1** provides the functions so authorised roles can manage the TSF data. This also defines each role's privileges for managing the TSF data. **FMT_SMF.1** provides security management of attributes and data to allow administration of the TOE. **FMT_SMR.1** specifies the four possible roles administrator, supervisor, operator and upgrader. **FTA_SSL.3** provides additional protection by automatically terminating management sessions after a period of user inactivity.

Objectives	SFRs
O.MGMT_PROTECT	**FCS_CKM.1/AES** specifies generation of AES keys which are used for control plane communications (SSH/SFTP, TLS/FTPS, SNMPv3). **FCS_CKM.1/ECDSA** specifies generation of ECDSA keys which are used in SSH and TLS. **FCS_CKM.2/DH** specifies Diffie Helman key exchange used in SNMPv3. **FCS_CKM.2/ECDH** specifies ephemeral key agreement used in TLS. **FCS_CKM.4/PK** requires destruction of above mentioned ECDSA keys. **FCS_CKM.4/AES** requires destruction of above mentioned AES keys. **FCS_COP.1/AES_Data** specifies AES encryption used in TLS, SSH and SNMPv3. **FCS_COP.1/SHA** specifies SHA used in TLS, SSH and SNMPv3. **FCS_COP.1/HMAC** specifies HMAC used in TLS, SSH and SNMPv3. **FCS_COP.1/ECDSA_sign** specifies ECDSA digital signatures used in SSH and TLS. **FMT_SMF.1** provides the capability for management of TOE security functions including control plane communications. **FTP_ITC.1/CP** requires use of trusted channels for communication with Key Servers and File Servers. **FTP_TRP.1** requires use of trusted paths for communication with remote administrators.
O.TRANSEC	**FDP_TSC_EXT.1** specifies TRANSEC capabilities. **FMT_SMF.1** provides the capability for management of TOE security functions including TRANSEC.
O.DEVICE_AUTH	**FCS_CKM.1/RSA, FCS_CKM.1/ECDSA, FCS_COP.1/RSA_sign and FCS_COP.1/ECDSA_sign** together with **FCS_COP.1/SHA** provide the means for signing completed X.509 certificates for the encryptor. **FDP_DAU.1** provides the means for producing a digest of the data for authentication purposes, when generating partial certificates in activation mode, and after sending completed activation data from CM7 to the encryptor. Activation provides secure replacement of the default user credentials. **FTP_ITC.1/ETH** provides the means for using the X.509 certificates to authenticate other encryptors and establish a secure trusted channel.

Objectives	SFRs
	FMT_SMF.1 provides the capability for management of TOE security functions.
O.AUDIT	**FAU_GEN.1** provides the capability for generating and recording audit events. **FAU_SAR.1** provides the capability for viewing audit logs. **FMT_SMF.1** provides the capability for management of TOE security functions. **FPT_STM.1** ensures that a date and time stamp is recorded with the audit record.
O.SECURE_STATE	**FPT_FLS.1 together with FPT_TST.1** provide the capability for the TOE to demonstrate correct operation by performing self-tests on start-up which ensures that the TOE will enter a secure state if any internal failure is detected. **FPT_PHP.3** requires that the TOE automatically responds to a physical tamper event to maintain a secure state.

7.3 TOE Summary Specification Rationale

84 Table 19 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 19: Map of SFRs to TSS Security Functions

	Ethernet Encryption	Transmission Security	Certificate Management	Cryptographic Operations	Secure Administration	Trusted Path/Channels	Self-Protection	Audit
FAU_GEN.1								X
FAU_SAR.1								X
FCS_CKM.1/AES				X				
FCS_CKM.1/RSA				X				
FCS_CKM.1/ECDSA				X				

	Ethernet Encryption	Transmission Security	Certificate Management	Cryptographic Operations	Secure Administration	Trusted Path/Channels	Self-Protection	Audit
FCS_CKM.2/RSA				X				
FCS_CKM.2/AES				X				
FCS_CKM.2/DH				X				
FCS_CKM.2/ECDH				X				
FCS_CKM.4/SMK				X				
FCS_CKM.4/PK				X				
FCS_CKM.4/AES				X				
FCS_COP.1/AES_Key				X				
FCS_COP.1/AES_Data				X				
FCS_COP.1/RSA_enc				X				
FCS_COP.1/SHA				X				
FCS_COP.1/HMAC				X				
FCS_COP.1/RSA_sign				X				
FCS_COP.1/ECDSA_sign				X				
FCS_SMC_EXT.1				X				
FDP_DAU.1			X					
FDP_ITC.2				X				
FDP_IFC.1/ETH	X							
FDP_IFF.1/ETH	X							
FDP_IFC.1/KEY				X				
FDP_IFF.1/KEY				X				

	Ethernet Encryption	Transmission Security	Certificate Management	Cryptographic Operations	Secure Administration	Trusted Path/Channels	Self-Protection	Audit
FDP_TSC_EXT.1		X						
FDP_UCT.1	X							
FIA_AFL.1					X			
FIA_UAU.2					X			
FIA_UID.2					X			
FMT_MSA.1					X			
FMT_MSA.3	X							
FMT_MTD.1			X		X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_FLS.1							X	
FPT_PHP.3							X	
FPT_STM.1								
FPT_TST.1							X	
FTA_SSL.3					X			
FTP_ITC.1/ETH	X							
FTP_ITC.1/CP						X		
FTP_TRP.1						X		