Senetas Corporation Ltd, distributed by Thales SA

CN Series Encryptors

Security Target

Table of contents

Table of figures

Table of tables

1. Security Target Introduction

This introductory chapter contains the following sections:

- Security Target Reference
- TOE Reference
- TOE Overview
- TOE Description
- TOE Life-cycle

1.1 ST Reference

Title	Senetas CN Series Security Target
Version	2.0
ST reference	CN_Series_ST_EAL4+_v2.0
Date	20-May-2021
Authors	Senetas
Evaluator	Oppida
Certification body	ANSSI

1.2 TOE Reference

The Target of Evaluation is identified as below:

Product Name	CN Series Ethernet Encryptors
Hardware Version	See Table 2 in Section 1.4.1 (TOE Product Family)
Firmware Version	5.0.2
Guidance	See Section 1.4.2 (Physical Scope)

Table 1. TOE Identification

1.3 TOE Overview

The TOE is a set of Senetas Ethernet encryptors (see Figure 1 - Figure 6), which are members of the Senetas CN Series encryptors. They are high-speed, standards-based encryptors designed to secure voice, data and video information transmitted over Ethernet networks. They also provide access control facilities using access rules for each defined Ethernet connection.

Figure 1: CN4010 1G Ethernet Encryptor

Figure 2: CN4020 1G Ethernet Encryptor

Figure 3: CN6010 1G Ethernet Encryptor

Figure 4: CN6140 1/10G Multi Port Ethernet Encryptor

Figure 5: CN9100 100G Ethernet Encryptor

Figure 6: CN9120 100G Ethernet Encryptor

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 either fibre optic or CAT5/6 cables. When operating at full bandwidth, the Ethernet encryptor will not discard any valid Ethernet frame in all modes of operation.

An operational overview of the CN6010 encryptor can be found in Figure 7.

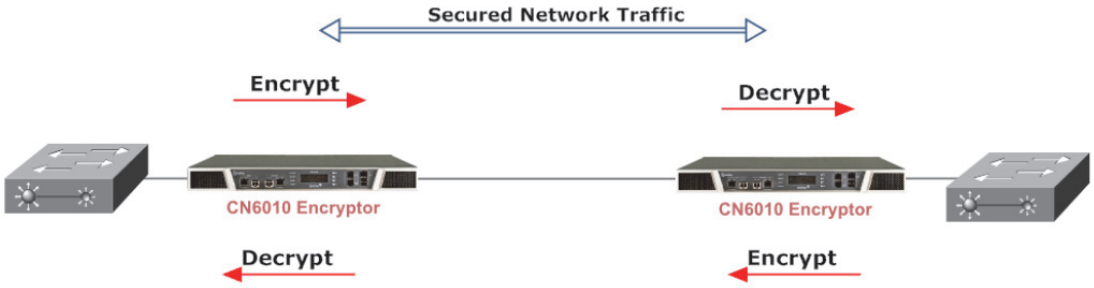

Figure 7: CN6010 operational overview

Different users' 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.

1.3.1 TOE Intended Usage

The TOE provides access control and protects the confidentiality and, optionally, the integrity of transmitted data between secured sites (e.g. data centers) by cryptographic mechanisms. The TOE supports three AES modes of operation (CTR, CFB and GCM), and the integrity of transmitted data is only ensured when the GCM operation mode is used.

The CN6140 model in 10G Multi port mode only supports the AES CTR mode, thus it can solely ensure the confidentiality (i.e. no integrity protection is provided) of the information transferred across the public network.

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

1.3.2 TOE Type

The TOE is a set of High-Speed Network Encryptors.

1.3.3 Non-TOE Hardware/Software/Firmware

The following hardware and software are not part of the TOE:

- The remote RS232 terminal used to connect to the encryptor CLI via the management RS232 port;
- The remote SSH terminal used to connect to the encryptor CLI via SSH;
- The remote TACACS+[1] authentication server;

[1] TACACS+ uses non-compliant algorithms and is considered to be out of scope of the certification. To be in a certified configuration TACACS+ should not be enabled.

- The CM7 remote management software application and the terminal on which it is running;
- The FTP server used for firmware upgrade;
- Quantum Key Distribution (QKD) unit;
- KeySecure server.

All of the encryptor hardware components are part of the TOE. In particular, the RS232 hardware on the encryptor side is part of the TOE. The SSH and CLI flows are also part of the TOE.

1.4 TOE Description

1.4.1 TOE product family

The family of Senetas ethernet encryptors considered in this security target includes:

- CN6010: the reference product
- CN6140[2] (4 modes of operation: 1G single-port, 1G Multi-port, 10G single-port and 10G Multi-port)
- CN4010
- CN4020
- CN9100
- CN9120

All these models share the same hardware architecture and the embedded software. Their differences (shown in Table 2) are only related to the physical interfaces, the data bandwidth and the supported AES modes of operation.

To ensure both confidentiality and the integrity of exchanged data frames, AES GCM mode must be used. The CTR and CFB operation modes only guarantee the confidentiality of the information transferred across the public network.

[2]The CN Series CN6140 model in 10G Multi port mode only ensures the confidentiality (i.e. no integrity protection is provided) of the information transferred across the public network

Model	HW Version	Power	FW Version	Protocol	AES Modes	I/F	LCD/ Keypad
CN4010	A4010B	DC (Plug Pack)	5.0.2	1G Ethernet	CFB, CTR, GCM	RJ45	No
CN4020	A4020B	DC (Plug Pack)	5.0.2	1G Ethernet	CFB, CTR, GCM	SFP	No
CN6010	A6010B A6011B A6012B	AC/AC Dual DC/DC Dual AC/DC Dual	5.0.2	1G Ethernet	CFB, CTR, GCM	RJ45, SFP	Yes
CN6140	A6140B A6141B A6142B	AC/AC Dual DC/DC Dual AC/DC Dual	5.0.2	1G Ethernet Single Port 1G Ethernet Multi Port	CFB, CTR, GCM	SFP+	Yes
				10G Ethernet Single Port	CTR, GCM		
				10G Ethernet Multi Port	CTR		
CN9100	A9100B A9101B A9102B	AC/AC Dual DC/DC Dual AC/DC Dual	5.0.2	100G Ethernet	CTR, GCM	CFP4	Yes
CN9120	A9120B A9121B A9122B	AC/AC Dual DC/DC Dual AC/DC Dual	5.0.2	100G Ethernet	CTR, GCM	QFSP28	Yes

Table 2. CN Series Product Family

As shown in Table 2, the GCM mode of operation is supported by all the CN Series encryptors except the CN6140 model in 10G Multi port mode. Consequently, the CN6140 model in 10G Multi port mode can only ensure the confidentiality (i.e. no integrity protection is provided) of the information transferred across the public network.

1.4.2 Physical Scope

The TOE reference product (i.e. CN6010) is composed of

- the CN6010 encryptor hardware device (refer to Table 3 below);
- the firmware (version 5.0.2);
- the guidance for the secure usage of the TOE:
  - Operational User Guidance [17]
  - Preparative Procedure [18]
  - User Guide [16]

ID	Description
A6010B	CN6010 1G ETHERNET (RJ45) AC UNIT
A6011B	CN6010 1G ETHERNET (RJ45) DC UNIT
A6012B	CN6010 1G ETHERNET (RJ45) AC/DC UNIT

Table 3. CN6010 Model Numbers

1.4.2.1 TOE physical interfaces

The TOE interfaces include local and network (private and public) data ports, providing connectivity between the secure and insecure network. These ports support electrical media

in the form of RJ45 electrical interfaces and SFP optical transceivers. Other ports consist of user access management ports (CLI via RS232 and SNMPv3 via Ethernet), LCD display, LEDs, USB, keypad port and erase port.

Table 4 sums up the interfaces of the TOE with the corresponding ports used and their usage.

Interface	Physical port	Use
Private network interface	Local port	The Local Port connects to the private network; access is protected by RSA and ECDSA certificates. The Local Port is of the same interface type as the Network Port.
Public network interface	Network port	The Network Port connects to the public network; access is protected by RSA and ECDSA certificates. The Network Port is of the same interface type as the Local Port.
Local console	RJ-45 RS-232 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 approved mode. This port also allows administrative access and monitoring of operations. User name and password authentication is required to access this port.
Keypad	Keypad	Allows entry of commands to display module configuration details.
Display	LCD + LEDs	Displays configuration information in response to commands entered via the navigation keypad.
Remote management interface	Management RJ-45 Ethernet port (LAN)	Allows secure and authenticated remote management via SNMPv3 by the selected remote management application.
Firmware upgrades	USB	The USB port provides a mechanism for applying approved and properly signed firmware upgrades to the module.
Deletion	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. The Erase feature can also be triggered using the Keypad (via a key press sequence).

Table 4. TOE Interfaces

1.4.3 Logical Scope

The TOE has the following two security features:

- Ethernet processing
- Secure management

1.4.3.1 Ethernet Processing

The TOE protects the Ethernet frame by encrypting the payload of the frame. The twelve-byte Ethernet frame header is unchanged, which enables switching off the frame through an

Ethernet network. The format of the Ethernet frame is shown in Figure 8. With the advent of gigabit Ethernet, jumbo frames of up to 10.000 bytes are also supported.

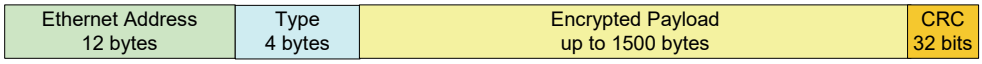

Figure 8: Ethernet frame format

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 transferred between encryptors encrypted using RSA-OAEP (in accordance with NIST SP 800-56B). Subsequent Data encrypting keys (DEKs) are transferred periodically between the encryptors encrypted using AES with the associated KEK and authenticated using HMAC-256. Alternatively, ECDSA/ECDH uses ephemeral key agreement for the purpose of establishing DEKs in accordance with NIST SP800-56A.

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.

The secure connection establishment protocol does not create an individually authenticated link between encryptors on the same network (the compromise of one encryptor can compromise the communications with all the other encryptors on the network). During secure connection establishment each encryptor is authenticated back to a common root trust anchor (CA).

The encryptors provide access control by discarding frames according to the access rules for that particular connection. Access controls may be set for any Unicast or Multicast Ethernet address or VLAN ID as encrypt, bypass or discard. Ethernet management frames can be selectively encrypted or passed through in bypass mode, thereby enabling Ethernet management functionality to be maintained.

1.4.3.2 Secure Management

Activation

Each encryptor must have the default user account credentials updated before any X.509 certificates can be installed. This process is referred to as activation, performed via CM7 (i.e. the management application), and validated by the administrator using the front panel display on the encryptor.

Alternatively a user can activate an encryptor by changing the default user account credentials by running the CLI "activate –l" command from the front panel console port.

Certification Authority

Each encryptor must have one or more X.509 certificates installed before the operation of the encryptor can start. Certificate signing requests are generated within the encryptor and extracted using CM7. Acting as the Certificate Authority, CM7 may sign this certificate locally, or the Certificate Signing Request (CSR) may be signed by an external CA. In either case, CM7 is used to install the signed certificate(s) into the encryptor.

Where certificates are not self-signed, multiple certificates may be required to establish the root trust anchor.

The CM7 management software is not part of the TOE.

Local Management

Local management is available via a RS232 port supporting a command line interface (CLI). Using a basic terminal emulator, a user is required to present their user name and authentication password directly to the encryptor before a local management session is allowed.

The RS232 terminal console is not part of the TOE.

Remote Management over SSH

The CLI can also be securely accessed remotely via SSH version 2 (when configured). The authentication algorithm for remote CLI access is restricted to ECDSA. ECDSA keys are restricted to NIST P-256, P-384 and P-521 curves. The user creates an SSH private/public key pair and installs their public key on the encryptor, which acts as the SSH server and their private key on the client computer.

Once SSH CLI is correctly configured on the encryptor the user can access the CLI remotely via SSH from the client computer using the username cli (e.g ssh cli@encryptor_ip_address). The SSH keys only grant access to the CLI login prompt. Once connected, the user is required to enter a valid user ID and password and the normal user authentication process is followed. Once validated the user will have the same privileges as if they were physically accessing the CLI via the front panel serial port.

Remote CLI access is disabled by default and cannot be enabled prior to the encryptor being activated.

The SSH terminal console is not part of the TOE.

Remote Management using SNMPv3

The CM7 management application, which uses SNMPv3 management sessions, and optionally acting as a CA, provides secure remote management of the Senetas encryptors. By default, CM7 enforces a user to have an authentication password for remote management sessions.

CM7, which must have IP connectivity to each encryptor in the network, can communicate via the dedicated Ethernet management port on the front of the encryptor, which supports a 10/100BaseT connection, or via the network interface ports for in-band management.

The CM7 management application is not part of the TOE.

Remote Management via TACACS+[3]

TACACS+ can be configured in the encryptor to allow Authentication, Authorization and Accounting (AAA) services to be provided from a remote TACACS+ server. TACACS+ is

[3] TACACS+ uses non-compliant algorithms and is considered to be out of scope of the certification. To be in a certified configuration TACACS+ should not be enabled

disabled by default. When this feature is enabled, TACACS+ requests are only sent when the given username does not exist within the local user table.

In line with the current role-based access control system, the TACACS+ server may be configured to provide one of four user access levels, providing the same level of control/access as for local users, i.e. ADMINISTRATOR/SUPERVISOR/OPERATOR/UPGRADER.

The remote TACACS+ authentication server is not part of the TOE.

1.4.3.3 TOE logical interfaces

The TOE logical interfaces include:

- SNMPv3 packets for remote management;
- Command line interface (CLI) for local management;
- SSH commands for remote management by CLI;
- Data frames to be processed;
- Secure Message Exchange (SME[4]) messages used for secure tunnel establishment between encryptors;
- FTP communications;
- QKD communications[5];
- KeySecure exchanges[5].

1.4.4 Forms of Delivery

The encryptor device is delivered with the embedded software.

1.4.5 TOE Life cycle

The TOE lifecycle is composed of the following phases.

Phase	Title	Description	Company	Location
1	TOE design	Hardware and (embedded) software development	Senetas	312 Kings Way, South Melbourne, Victoria 3205, Australia
2	TOE manufacturing	Hardware manufacturing and testing	Extel	399 Ferntree Gully Road, Mount Waverley, Victoria 3149, Australia
3	TOE finalization and delivery	Load of final (embedded) software; Software testing; Delivery;	Senetas	312 Kings Way, South Melbourne, Victoria 3205, Australia

Table 5. TOE Life-cycle

[4] Senetas proprietary protocol
[5] QKD and KeySecure communications are interfaces of the TOE, but are not TSFIs.

2. Conformance Claim

This chapter contains the following sections:

- CC Conformance Claim
- PP Claim
- Package Claim
- Conformance Claim Rationale

2.1 CC Conformance Claim

This Security target claims to be conformant to the Common Criteria version 3.1 Release 5 ([1], [2], [3], [4]).

Furthermore, it claims to be CC Part 2 and CC Part 3 strict conformant.

2.2 PP Claim

This Security Target does not claim conformance to any Protection Profile.

2.3 Package Claim

The assurance level for this Security Target is EAL4 augmented with ALC_FLR.3.

2.4 Conformance Claim Rationale

Not applicable.

3. Security Problem Definition

3.1 Assets

D.MASTER_KEY

A 256-bit symmetric key generated on initialization. D.MASTER_KEY is stored in a tamper protected non-volatile (battery backed) RAM, and is zeroized on Tamper or Extended Factory Erase. A CRC is stored along with the D.MASTER_KEY key (in non-volatile RAM) in order to ensure its integrity.

D.MASTER_KEY is used to encrypt the RSA and ECDSA private keys as well as the user password data, using AES-256 CFB.

D.MASTER_KEY is protected in confidentiality and integrity.

D.RSA_KEYS

The public key is stored in the network certificate and used for authenticating connections with other encryptors. The private key is used to authenticate connections with other encryptors and unwrap master session keys (KEK) and initial Data Encryption Key (DEK) received from far-end encryptors.

D.RSA_KEY private key is protected in confidentiality. The public key is protected in integrity.

D.CERTIFICATE

Each encryptor is bound to one or more X.509 certificates signed by Certificate Authorities (CAs).

D.CERTIFICATE is protected in integrity.

D.USR_PWD

The password of a user.

D.USR_PWD is protected in confidentiality and integrity.

D.KEK

Key Encrypting Key is used to protect D.DEK that is changed periodically.

D.KEK is protected in confidentiality and integrity.

D.DEK

DEK stands for Data Encrypting Key. Those are AES keys used for encrypting and decrypting the user data transferred between the Encryptors. They are changed periodically and are transferred in an encrypted form (using a KEK).

D.DEK is protected in confidentiality and integrity.

D.PRIVACY_KEY

An AES key used to encrypt the SNMPv3 data packets during the remote management session.

D.PRIVACY_KEY is protected in confidentiality and integrity.

D.ECDSA_KEYS

The public key is stored in the network certificate and used for authenticating connections with other encryptors. The private key is used to authenticate connections with other encryptors.

D.ECDSA_KEYS private key is protected in confidentiality. The public key is protected in integrity.

D.USR_DATA

Data transfered between encryptors.

D.USR_DATA is protected in confidentiality (regardless of the used AES mode of operation) and integrity (provided that the AES GCM mode of operation is supported[6] and used).

D.MANAGEMENT_DATA

Data received by the encryptor for management purposes.

D.MANAGEMENT_DATA is protected in confidentiality and integrity.

D.ENCRYPTOR_TIME

Date and time of the encryptor.

D.ENCRYPTOR_TIME is protected in integrity.

D.LOGS

The encryptor maintains two separate logs, namely an audit log (recording all configuration changes made to the encryptor) and an event log (recording significant events that happen, such as self-tests results).

D.LOGS is protected in integrity.

D.ENCRYPTOR_CONFIG

Encryptor configuration data.

D.ENCRYPTOR_CONFIG is protected in integrity.

3.2 Users / Subjects

S.Host

S.Host represents external and internal hosts which send and receive information through the TOE.

U.Administrator

Administrators have full access rights.

[6] Note that the CN Series CN6140 model in 10G Multi port mode only supports the AES CTR mode of operation, which only ensures the confidentiality (i.e. no integrity protection) of the data transferred between encryptors. Refer to Table 2 for further details on the supported modes.

U.Supervisor

Supervisors have full access rights except that they cannot

- add, delete or modify the user accounts
- install X509 certificates
- upgrade the firmware

U.Operator

Operators can view all available information but cannot delete, add or modify the information.

U.Upgrader

Upgraders can apply firmware upgrades and can view all available information but cannot delete, add or modify the information.

3.3 Threat agents

The threats described in the following chapter consider the following threat agents:

- Authorised user: a legitimate user of the TOE, i.e. U.Administrator, U.Supervisor, U.Operator or U.Supervisor;
- Insider attacker: an attacker located in the private network trying to compromise the confidentiality and/or integrity of the TOE assets. An insider attacker may be an authorised user;
- Outsider attacker: an attacker located in the public network trying to compromise the confidentiality and/or integrity of the TOE assets.

3.4 Threats

T.ILLEGAL_DATA_ACCESS

Data being transmitted across a public Ethernet data network may be illegitimately modified[7] or disclosed to an outsider attacker or authorised user of the TOE through malfunction of the TOE.

Related assets: D.USR_DATA, D.MANAGEMENT_DATA

T.UNAUTHORIZED_CONNECTION

An attacker (insider or outsider) may attempt to make unauthorised connections to another Ethernet data network and transmit information, which was to be kept confidential, to another destination.

Related assets: D.USR_DATA, D.MANAGEMENT_DATA

T.IMPERSON

An attacker (outsider or insider) may impersonate an authorised user of the TOE to gain access to information that was to be kept confidential, and/or to alter TOE assets.

[7] Transmitted data modification is only considered when the AES GCM mode of operation is supported and used. Refer to Table 2 for further details on the AES supported modes.

Related assets: D.MASTER_KEY, D.RSA_KEYS, D.CERTIFICATE, D.USR_PWD, D.KEK, D.DEK, D.PRIVACY_KEY, D.ECDSA_KEYS, D.USR_DATA, D.ENCRYPTOR_TIME, D.LOGS, D.MANAGEMENT_DATA, D.ENCRYPTOR_CONFIG

T.LINK_INFORMATION

An attacker (outsider or insider) may be able to observe multiple uses of services by an entity. By linking these uses, the individual may be able to deduce information, which the entity wishes to keep confidential.

Related assets: D.RSA_KEYS, D.KEK, D.DEK, D.PRIVACY_KEY, D.ECDSA_KEYS, D.USR_DATA, D.MANAGEMENT_DATA

T.PHYSICAL_ATTACK

Security critical parts of the TOE may be subject to physical attack by an (outsider or insider) attacker, which may compromise security.

Related assets: D.MASTER_KEY, D.RSA_KEYS, D.CERTIFICATE, D.USR_PWD, D.KEK, D.DEK, D.PRIVACY_KEY, D.ECDSA_KEYS, D.USR_DATA, D.MANAGEMENT_DATA, D.LOGS, D.ENCRYPTOR_CONFIG, D.ENCRYPTOR_TIME

T.UNIT_COMPROMISE

An attacker has compromised an encryptor and can decrypt all other communications of the other encryptors within the network

Related assets: D.MASTER_KEY, D.RSA_KEYS, D.CERTIFICATE, D.KEK, D.DEK, D.PRIVACY_KEY, D.ECDSA_KEYS

3.5 Organisational Security Policies

P.CRYPTOGRAPHIC_OPERATIONS

All encryption services, including confidentiality, authentication and key management, must conform to standards specified in FIPS PUB 140-2 [15].

P.FLOW

Traffic flow is controlled on the basis of the information in the Ethernet frame and the action specified in the Connection Identifier Table. Any frame for which there is no CI entry is discarded by default.

By default, all Ethernet frames are discarded.

P.ROLES

Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users (U.Administrators, U.Supervisors, U.Operator and U.Upgrader).

3.6 Assumptions

A.LOCATE

It is assumed that the encryptor is located in a secure area at the boundary of the site to be protected. This is required to ensure that the unit is not physically bypassed.

A.SECURE_INSTALLATION

It is assumed that the end-user will provide adequate physical and organizational protection of the encryptors to prevent theft and misuse.

A.ADMIN

It is assumed that U.Administrator, U.Supervisor, U.Operator and U.Upgrader assigned as authorised users, are competent to manage the TOE, and can be trusted not to deliberately abuse their privileges so as to undermine security.

A.AUDIT

It is assumed that appropriate audit and event logs are maintained and regularly examined. Without capturing security relevant events or performing regular examination of audit records, a compromise of security may go undetected.

A.INSTALL

It is assumed that the encryptor is installed on the boundary of the protected and unprotected network. The encryptor needs to be installed on the boundary to ensure confidentiality of transmitted information.

A.TIME

It is assumed that the encryptor RTC is initially configured with a correct date and time. In the case where an NTP server is configured, it is assumed that it provides reliable timestamps.

A.CA

It is assumed that the Certification Authority is trustworthy.

A.MANAGEMENT_TERMINAL

It is assumed that the terminal used for the remote management of the encryptor is trustworthy.

A.CM7

It is assumed that the CM7 software can only be used by authorised users, and is trustworthy (i.e. operates in a secure environment and in correct way).

A.FTP_SERVER

It is assumed that the FTP server (used for firmware upgrade) is trustworthy and securely configured.

4. Security Objectives

4.1 Security Objectives for the TOE

O.AUDIT

The TOE must provide a means to record a readable audit trail of security relevant events with accurate dates and times so as to assist in the detection of potential attacks of the TOE and also to hold users accountable for any actions that they perform.

O.CERT_MANAGEMENT

The TOE must provide the means for requesting and managing signed X.509 certificates that conform to the standards specified in FIPS PUB 140-2 [15]. The TOE must use the X.509 certificates to authenticate other encryptors in order to establish a secure trusted channel between encryptors.

O.DATA_PROTECTION

The TOE must provide the means of protecting the confidentiality and the integrity (provided that the AES GCM mode of operation is supported[8] and used) of the information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB 140-2 [15].

O.SECURE_STATE

In the event of an error occurring, the TOE will preserve a secure state.

O.FLOW

The TOE must provide authorised users with the means of controlling traffic flow received and transmitted on the local and network interfaces, on the basis of header information, in accordance with the set of rules defined in P.FLOW. This includes bypassing, discarding or encrypting operations.

O.KEY_MANAGEMENT

The TOE must provide the means for secure management of cryptographic keys. This includes generating, distributing, agreeing, encrypting, destroying and exchanging keys with only another authorised TOE or a remote trusted IT product so the key exchange conforms to standards specified in FIPS PUB 140-2 [15].

O.REMOTE_MANAGEMENT

The TOE must allow secure remote management of the TOE using cryptographic measures that conforms to standards specified in FIPS PUB 140-2 [15].

[8] The CN6140 encryptor in 10G Multi-port mode does not support AES GCM mode of operation and, thus, cannot ensure the integrity of the transferred information. It only guarantees the confidentiality of the exchanged data. Refer to Table 2 for further details on the supported modes.

O.ROLE_MANAGEMENT

The TOE must uniquely identify all users and authenticate the claimed identity before granting a user access to the TOE management facilities.

The TOE must provide functionality, which enables an authorised user to effectively manage the TOE and its security functions, and must ensure that only authorised users are able to access such functionality, while also maintaining confidentiality of sensitive management data.

The TOE must prevent users from gaining access to and performing operations, on its resources for which their role is not explicitly authorised.

4.2 Security Objectives for the Operational Environment

OE.AUDIT_LOG

Authorised TOE users must ensure that audit facilities are used and managed effectively. In particular:

- Appropriate action must be taken to ensure the continuous audit logging, e.g. by regular archiving of logs.
- Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

OE.PERSONNEL

Authorised TOE user is competent and can be trusted not to deliberately abuse his or her privileges to undermine security.

TOE users must ensure the secure operation of the TOE. More precisely, they shall ensure

- the secure storage of the authentication data for each account on the TOE
- the non-disclosure of authentication data to persons unauthorised to use that account
- no connection to outside systems or users that would undermine IT security
- the security during the delivery, installation, management and operation of the TOE.

U.Administrator with responsibility for controlling who has access to the unit for configuration and monitoring activities must allocate user roles with the concept of least privilege.

OE.PHYSICAL_PROTECTION

Critical parts of the TOE are protected from physical attack, which might compromise IT security. TOE users must also ensure that the Certificate Authority (CA) is protected from physical attacks.

OE.SETUP_AND_INSTALL

TOE users must ensure that no connections are provided to outside systems or users that would undermine IT security.

TOE users must ensure that the TOE is delivered, installed, managed and operated in a manner which maintains IT security.

OE.RELIABLE_TIME

The encryptor RTC must be configured with a correct date and time. If an NTP server is configured, it must be ensured that it provides reliable and correct timestamps.

OE.CA

It must be ensured that the Certification Authority is trustworthy and protected from physical attacks. In particular, the CA must only provide signed certificates to legitimate encryptors.

OE.MANAGEMENT

The management terminal and the CM7 management software must be trustworthy and operate in a secure environment (i.e. protected from physical attacks). They shall only be accessed by authorised users.

OE.FTP_SERVER

It must be ensured that the FTP server is securely configured (e.g. use of strong authentication, encryption and hashing primitives) using either SFTP or FTPS protocols.

4.3 Security Objectives Rationale

4.3.1 Threats

T.ILLEGAL_DATA_ACCESS O.DATA_PROTECTION ensures that the information transferred across a public network is protected by cryptographic mechanisms.

O.FLOW ensures that the information is not sent to an unauthorized encryptor.

O.KEY_MANAGEMENT ensures that the cryptographic keys used in O.DATA_PROTECTION are not disclosed to an unauthorized encryptor.

O.SECURE_STATE ensures that the TOE will enter a secure state if any malfunction of the TOE is detected.

OE.FTP_SERVER ensures that firmware update images are protected in terms of confidentiality and integrity during their download.

T.UNAUTHORIZED_CONNECTION O.CERT_MANAGEMENT, OE.RELIABLE_TIME and OE.CA ensure that an encryptor without a valid certificate cannot establish a secure channel with another encryptor.

O.FLOW ensures that the information is not sent to an unauthorized encryptor.

O.KEY_MANAGEMENT ensures that the cryptographic keys used in O.DATA_PROTECTION are not disclosed to an unauthorized encryptor.

OE.PERSONNEL ensures that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account.

T.IMPERSON O.ROLE_MANAGEMENT ensures that users are allocated roles with least privilege and a user can only access the operations that the role authorises. It also ensures that all users are uniquely identified and authenticated before access to the TOE management features is allowed.

O.REMOTE_MANAGEMENT and OE.MANAGEMENT ensure that the remote management of the TOE is secure.

OE.PERSONNEL ensures that the authentication data for each account is held securely and not disclosed to persons unauthorised to use that account. Therefore, if the audit trail indicates an abuse by a certain role, then the human allocated that role can be held responsible for those actions. This, in conjunction with abuse detection (O.AUDIT and OE.AUDIT_LOG), will deter users from intentionally abusing their privileges. It also ensures that only trusted and competent personnel operate the TOE. A trusted user will not intentionally abuse their privileges, while a competent user will not accidentally perform operations that compromise information.

OE.SETUP_AND_INSTALL enforces the responsibility of the users during the usage of the encryptor.

O.ROLE_MANAGEMENT and OE.FTP_SERVER ensure that only TOE administrators and upgraders can remotely access the FTP server and download new firmware (using FTPS or SFTP) to perform firmware upgrades.

T.LINK_INFORMATION O.FLOW allows authorized users to explicitly allow connections (all connections to the TOE being discarded by default).

O.DATA_PROTECTION ensures that the data transferred between encyptors is protected.

O.KEY_MANAGEMENT provides the means for exchanging keys with only other authorised encryptors to establish a link. The other encryptors are only authorised due to X.509 certificate attributes as provided by O.CERT_MANAGEMENT and OE.CA. Therefore O.KEY_MANAGEMENT, O.CERT_MANAGEMENT, OE.CA and OE.RELIABLE_TIME restrict the number of possible communication paths to only other authorised encryptors.

The objectives O.FLOW, O.KEY_MANAGEMENT, OE.CA, OE.RELIABLE_TIME and O.CERT_MANAGEMENT combine to minimise the number of communication links that an encryptor will have. The minimal links will reduce the opportunity an attacker has to deduce information. As confidential information over these links will be encrypted due to O.DATA_PROTECTION, the attacker will require more resources and knowledge to deduce any useful information. Therefore the combination of all these objectives will lower this threat to an acceptable level.

T.PHYSICAL_ATTACK OE.PERSONNEL ensures that TOE users are competent to manage the TOE and can be trusted not to deliberately abuse their privileges. OE.PHYSICAL_PROTECTION ensures that those parts of the TOE that are critical to security policy enforcement are protected from physical attacks. OE.CA, OE.MANAGEMENT ensures that non-TOE parts are protected from physical attacks. OE.SETUP_AND_INSTALL ensures that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.

T.UNIT_COMPROMISE OE.PERSONNEL ensures that TOE users are competent to manage the TOE and can be trusted not to deliberately abuse their privileges. OE.PHYSICAL_PROTECTION ensures that those parts of the TOE that are critical to security policy enforcement are protected from physical attacks. OE.SETUP_AND_INSTALL ensures

that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.

4.3.2 Organisational Security Policies

P.CRYPTOGRAPHIC_OPERATIONS O.DATA_PROTECTION, O.KEY_MANAGEMENT, O.REMOTE_MANAGEMENT and O.CERT_MANAGEMENT provide the confidentiality, authentication and key management services specified by this organisational security policy.

P.FLOW O.FLOW provides the traffic flow control specified in the organisational security policy.

O.ROLE_MANAGEMENT ensures that only authorised users can set the traffic control as specified in the organisational security policy.

P.ROLES O.ROLE_MANAGEMENT ensures that administrators will allocate users to distinct roles on the basis of least privilege and that users can only perform the operations for which their role is explicitly authorised.

OE.PERSONNEL and OE.FTP_SERVER ensure that only authorised users can manage the TOE as specified in the organisational security policy.

4.3.3 Assumptions

A.LOCATE OE.SETUP_AND_INSTALLATION ensures that encryptors are installed correctly in a secure environment while OE.PHYSICAL_PROTECTION ensures that this environment remains secure from unauthorised people.

OE.PERSONNEL ensures that only trusted and competent administrators are authorised to manage the TOE.

A.SECURE_INSTALLATION OE.SETUP_AND_INSTALLATION ensures that encryptors are installed correctly in a secure environment while OE.PHYSICAL_PROTECTION ensures that this environment remains secure from unauthorised people.

OE.PERSONNEL ensures that only trusted and competent administrators are authorised to manage the TOE.

A.ADMIN OE.PERSONNEL ensures that only trusted and competent administrators are authorised to manage the TOE.

A.AUDIT OE.AUDIT_LOG ensures that the facilities to effectively manage audit information are provided.

A.INSTALL OE.SETUP_AND_INSTALLATION ensures that the TOE is delivered, installed, managed and operated in a manner that maintains security.

OE.PERSONNEL ensures that only trusted and competent administrators are authorised to manage the TOE.

A.TIME OE.RELIABLE_TIME ensures that the TOE provides reliable and correct timestamps.

A.CA OE.CA ensures that the Certification Authority is trustworthy.

A.MANAGEMENT_TERMINAL OE.MANAGEMENT ensures that the management terminal is trustworthy.

A.CM7 OE.MANAGEMENT ensures that the CM7 management software is trustworthy, is installed in a secure environment and can only be accessed by authorised people.

A.FTP_SERVER OE.FTP_SERVER ensures that the FTP server is appropriately secured and configured, thus ensuring that firmware upgrades are properly protected in terms of confidentiality and integrity. In particular, the interface with the FTP server will not impact the security of the TOE.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.ILLEGAL_DATA_ACCESS	O.DATA_PROTECTION, O.FLOW, O.KEY_MANAGEMENT, O.SECURE_STATE, OE.FTP_SERVER	Section 4.3.1
T.UNAUTHORIZED_CONNECTION	O.CERT_MANAGEMENT, O.FLOW, O.KEY_MANAGEMENT, OE.PERSONNEL, OE_RELIABLE_TIME, OE_CA	Section 4.3.1
T.IMPERSON	O.AUDIT, OE.AUDIT_LOG, O.ROLE_MANAGEMENT, OE.MANAGEMENT, OE.PERSONNEL, OE.FTP_SERVER, OE.SETUP_AND_INSTALL, O.REMOTE_MANAGEMENT	Section 4.3.1
T.LINK_INFORMATION	O.CERT_MANAGEMENT, O.DATA_PROTECTION, O.FLOW, O.KEY_MANAGEMENT, OE.CA, OE.RELIABLE_TIME	Section 4.3.1
T.PHYSICAL_ATTACK	OE.PERSONNEL, OE.MANAGEMENT, OE.PHYSICAL_PROTECTION, OE.CA, OE.SETUP_AND_INSTALL	Section 4.3.1
T.UNIT_COMPROMISE	OE.PERSONNEL, OE.PHYSICAL_PROTECTION, OE.SETUP_AND_INSTALL	Section 4.3.1

Table 6. Threats and Security Objectives – Coverage

Security Objectives	Threats
O.AUDIT	T.IMPERSON
O.CERT_MANAGEMENT	T.UNAUTHORIZED_CONNECTION, T.LINK_INFORMATION
O.DATA_PROTECTION	T.ILLEGAL_DATA_ACCESS, T.LINK_INFORMATION
O.SECURE_STATE	T.ILLEGAL_DATA_ACCESS
O.FLOW	T.ILLEGAL_DATA_ACCESS, T.UNAUTHORIZED_CONNECTION, T.LINK_INFORMATION
O.KEY_MANAGEMENT	T.ILLEGAL_DATA_ACCESS, T.UNAUTHORIZED_CONNECTION, T.LINK_INFORMATION
O.REMOTE_MANAGEMENT	T.IMPERSON
O.ROLE_MANAGEMENT	T.IMPERSON
OE.AUDIT_LOG	T.IMPERSON
OE.PERSONNEL	T.UNAUTHORIZED_CONNECTION, T.IMPERSON, T.PHYSICAL_ATTACK, T.UNIT_COMPROMISE
OE.PHYSICAL_PROTECTION	T.PHYSICAL_ATTACK, T.UNIT_COMPROMISE
OE.SETUP_AND_INSTALL	T.IMPERSON, T.PHYSICAL_ATTACK, T.UNIT_COMPROMISE
OE.RELIABLE_TIME	T.UNAUTHORIZED_CONNECTION, T.LINK_INFORMATION,
OE.CA	T.UNAUTHORIZED_CONNECTION, T.LINK_INFORMATION, T.PHYSICAL_ATTACK
OE.MANAGEMENT	T.IMPERSON, T.PHYSICAL_ATTACK
OE.FTP_SERVER	T.ILLEGAL_DATA_ACCESS, T.IMPERSON

Table 7. Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CRYPTOGRAPHIC_OPERATIONS	O.CERT_MANAGEMENT, O.KEY_MANAGEMENT, O.REMOTE_MANAGEMENT, O.DATA_PROTECTION	Section 4.3.2
P.FLOW	O.FLOW, O.ROLE_MANAGEMENT	Section 4.3.2
P.ROLES	O.ROLE_MANAGEMENT, OE.FTP_SERVER OE.PERSONNEL	Section 4.3.2

Table 8. OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
O.AUDIT	
O.CERT_MANAGEMENT	P.CRYPTOGRAPHIC_OPERATIONS
O.DATA_PROTECTION	P.CRYPTOGRAPHIC_OPERATIONS
O.SECURE_STATE	
O.FLOW	P.FLOW
O.KEY_MANAGEMENT	P.CRYPTOGRAPHIC_OPERATIONS
O.REMOTE_MANAGEMENT	P.CRYPTOGRAPHIC_OPERATIONS
O.ROLE_MANAGEMENT	P.FLOW, P.ROLES
OE.AUDIT_LOG	
OE.PERSONNEL	P.ROLES
OE.PHYSICAL_PROTECTION	
OE.SETUP_AND_INSTALL	
OE.RELIABLE_TIME	
OE.CA	
OE.MANAGEMENT	
OE.FTP_SERVER	P.ROLES

Table 9. Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.LOCATE	OE.PHYSICAL_PROTECTION, OE.PERSONNEL, OE.SETUP_AND_INSTALL	Section 4.3.3
A.SECURE_INSTALL	OE.PHYSICAL_PROTECTION, OE.PERSONNEL, OE.SETUP_AND_INSTALL	Section 4.3.3
A.ADMIN	OE.PERSONNEL	Section 4.3.3
A.AUDIT	OE.AUDIT_LOG	Section 4.3.3
A.INSTALL	OE.PERSONNEL, OE.SETUP_AND_INSTALL	Section 4.3.3
A.TIME	OE.RELIABLE_TIME	Section 4.3.3
A.CA	OE.CA	Section 4.3.3
A.MANAGEMENT_TERMINAL	OE.MANAGEMENT	Section 4.3.3
A.CM7	OE.MANAGEMENT	Section 4.3.3
A.FTP_SERVER	OE.FTP_SERVER	Section 4.3.3

Table 10. Assumptions and Security Objectives for the Operational Environment – Coverage

Security Objectives for the Operational Environment	Assumptions
OE.AUDIT_LOG	A.AUDIT
OE.PERSONNEL	A.LOCATE, A.ADMIN, A.INSTALL, A.SECURE_INSTALL
OE.PHYSICAL_PROTECTION	A.LOCATE, A.SECURE_INSTALL
OE.SETUP_AND_INSTALL	A.LOCATE, A.INSTALL, A.SECURE_INSTALL
OE.RELIABLE_TIME	A.TIME
OE.CA	A.CA
OE.MANAGEMENT	A.MANAGEMENT_TERMINAL A.CM7
OE.FTP_SERVER	A.FTP_SERVER

Table 11. Security Objectives for the Operational Environment and Assumptions - Coverage

5. Security Requirements

5.1 Overview

This chapter describes the security functional and assurance requirements which have to be fulfilled by the TOE.

The following notations are used:

- **Selection** operation (denoted by *italic* text): used to select one or more options in stating a requirement;
- **Assignment** operation (denoted by **bold** *text)*: used to assign a specific value to an unspecified parameter, such as the size of a key;
- **Iteration** operation: are identified with a suffix in the name of the SFR (e.g. FCS_CKM.1/AES)

The security functional requirements refer to the the following:

- Subjects:
  - S.HOST (see Section 3.2);
  - Administrators.
- Objects:
  - Ethernet frames, received and sent by the TOE through the local and network interfaces;
  - X.509 activation Certificate generation requests from an encryptor;
  - new X.509 activation Certificates generated by CM7 for an encryptor.
- Operations:
  - Encrypt
  - Bypass
  - Discard
- Security attributes[9]:
  - MAC address for Ethernet information flows
  - VLAN ID for Ethernet information flows

[9] Note that the iSID connection mode is out of the scope of the certification. To be in a certified configuration, the iSID mode should not be used.

5.2 Security Functional Requirements

5.2.1 FAU: Security audit

FAU_GEN.1 Audit data generation

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 *minimum* level of audit; and

c)

- **FMT_MTD.1 All modifications to the values of the TSF data**
- **FPT_FLS.1 Failure of the TSF.**
- **FPT_TST.1 Execution of the TSF self tests and the results of the tests.**

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,

- **FCS_CKM.1/RSA Success and failure of the activity**
- **FCS_CKM.1/ECDSA Success and failure of the activity**
- **FCS_CKM.2/RSA Success and failure of the activity**
- **FCS_CKM.2/AES Success and failure of the activity**
- **FCS_CKM.2/ECDSA Success and failure of the activity**
- **FCS_CKM.2/ECDH Success and failure of the activity**
- **FCS_CKM.4/SMK Success and failure of the activity**
- **FCS_CKM.4/PK Success and failure of the activity**
- **FCS_CKM.4/AES Success and failure of the activity**
- **FCS_COP.1/RSA_enc Success and failure**
- **FCS_COP.1/ECDSA_enc Success and failure**
- **FCS_COP.1/SHA Success and failure**
- **FCS_COP.1/RSA_Sign Success and failure**
- **FCS_COP.1/ECDSA_Sign Success and failure**
- **FDP_DAU.1 Successful generation of validity evidence**
- **FDP_IFF.1 Decisions to permit requested information flows.**
- **FDP_UCT.1 The identity of any user or subject using the data exchange mechanism**
- **FIA_AFL.1 The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.**
- **FMT_SMR.1 Modifications to the group of users that are part of a role**
- **FPT_STM.1 Changes to the time**

- **FTA_SSL.3 Termination of an interactive session by the session locking mechanism**

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **U.Administrator, U.Supervisor, U.Operator and U.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.

5.2.2 FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

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 and surpassed*, the TSF shall **disable the user account for three minutes**.

FIA_UAU.2 User authentication before any action

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_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **a local password based authentication mechanism** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **local password based authentication mechanism**.

FIA_UID.2 User identification before any action

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.

5.2.3 FDP: User Data protection

FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **activation Certificate generation requests from an encryptor and new activation Certificates 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_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Information Flow Control SFP** on

Subjects: S.Host

Objects: Ethernet frames

Operation: Encrypt, bypass or discard.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Information Flow Control SFP** based on the following types of subject and information security attributes:

- **MAC address contained in the Ethernet frame header in MAC mode and**
- **VLAN ID contained in the Ethernet frame header in VLAN mode**.

FDP_IFF.1.2 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 is listed in the CI, then the defined operation in the CI is allowed**.

FDP_IFF.1.3 The TSF shall enforce the **additional information flow control 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 The TSF shall explicitly authorise an information flow based on the following rules: **none**.

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

FDP_UCT.1 Basic data exchange confidentiality

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

5.2.4 FCS: Cryptographic support

5.2.4.1 CKM

FCS_CKM.1/AES Cryptographic key generation

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**.

Application Note:

AES keys are used to protect stored X.509 certificates, RSA/ECDSA private keys and user account passwords as well as user data during transmission.

FCS_CKM.1/RSA Cryptographic key generation

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: **PKCS #1**.

Application Note:

The Encryptor can generate RSA or ECDSA keys.

FCS_CKM.1/ECDSA Cryptographic key generation

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**.

Application Note:

The Encryptor can generate RSA or ECDSA keys.

FCS_CKM.2/RSA Cryptographic key distribution

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

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/ECDSA Cryptographic key distribution

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

FCS_CKM.4/SMK Cryptographic key destruction

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**.

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.

FCS_CKM.4/PK Cryptographic key destruction

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

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_CKM.2/DH Cryptographic key distribution

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

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.

5.2.4.2 COP

FCS_COP.1/AES_Key Cryptographic operation

FCS_COP.1.1/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

FCS_COP.1.1/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[10] or NIST SP800-38D[11]**.

[10] For CFB and CTR modes of operation
[11] For GCM mode of operation

FCS_COP.1/RSA_enc Cryptographic operation

FCS_COP.1.1/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**.

Application Note:

The Encryptor can use 2048 bit RSA keys and P-256, P-384 or P-521 elliptic curves.

FCS_COP.1/ECDSA_enc Cryptographic operation

FCS_COP.1.1/ECDSA_enc The TSF shall perform **public key encryption** in accordance with a specified cryptographic algorithm **ECDSA/ECDH ephemeral key agreement** and cryptographic key sizes **P-256, P-384 and P-521** that meet the following: **NIST SP800-56A**.

Application Note:

The Encryptor can use 2048 bit RSA keys and P-256, P-384 or P-521 elliptic curves.

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **message digest generation/verification** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **256 bits** that meet the following: **FIPS PUB 180-4**.

FCS_COP.1/RSA_sign Cryptographic operation

FCS_COP.1.1/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**.

Application Note:

The Encryptor can use 2048 bit RSA keys and P-256, P-384 or P-521 elliptic curves.

FCS_COP.1/ECDSA_sign Cryptographic operation

FCS_COP.1.1/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 Digital Signature Standard**.

Application Note:

The Encryptor can use 2048 bit RSA keys and P-256, P-384 or P-521 elliptic curves.

5.2.5 FMT: Security Management

FMT_MSA.1 Management of security attributes

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

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Information Access Control 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

FMT_MTD.1.1 The TSF shall restrict the ability to

- *change_default, query, modify, delete and clear* the **CI table, User Account table, X.509 certificate** to **U.Administrator**
- *change_default, modify, delete and clear* the **CI table** to **U.Supervisor**
- *query* the **User Account table** to **U.Supervisor**
- *query* the **CI and User Account tables** to **U.Operator, U.Supervisor and U.Administrator**
- *clear* the **audit log** to **U.Administrator**
- *set* the **system time** to **U.Administrator and U.Supervisor**

FMT_SMF.1 Specification of Management Functions

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

- **security attribute management**
- **TSF data management**.

FMT_SMR.1 Security roles

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

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

5.2.6 FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

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_STM.1 Reliable time stamps

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

FPT_TST.1 TSF testing

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.*

5.2.7 FTA: TOE access

FTA_SSL.3 TSF-initiated termination

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

5.2.8 FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 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 The TSF shall permit *the TSF and another trusted IT product* to initiate communication via the trusted channel.

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

5.3 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_FLR.3.

5.4 Security Requirements Rationale

5.4.1 Objectives

5.4.1.1 Security Objectives for the TOE

O.AUDIT FAU_GEN.1 provides the capability for generating and recording audit events in the manner required by O.AUDIT.

FAU_SAR.1 provides the capability for viewing audit logs to support the effective use and management of the audit facilities in a manner required by O.AUDIT.

FPT_STM.1 ensures that a date and time stamp is recorded with the audit record. If the user sets a timezone other than UTC then the following procedure should be applied to guarantee the accuracy of time stamps. Set the time to UTC time and then change the timezone to the required location.

O.CERT_MANAGEMENT FCS_COP.1/RSA_enc and FCS_COP.1/ECDSA_enc use the RSA and ECDSA algorithms respectively to securely transfer symmetric encryption keys between encryptors (RSA is used for key encapsulation and authentication. ECDSA is only used for signing and authentication. ECDH is used for key agreement).

FCS_COP.1/AES_Key provides an additional encryption of the private keys that are stored in non-volatile memory.

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. These cryptographic functions meet the standards required by FIPS 140-2 [15].

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 and signed certificates from CM7 to the encryptor. Activation provides secure replacement of the default user credentials.

FTP_ITC.1 provides the means for using the X.509 certificates to authenticate other encryptors and establish a secure trusted channel.

O.DATA_PROTECTION FCS_COP.1/AES_Data and FDP_UCT.1 provide the capability for encrypting information to protect the confidentiality and integrity of the information transferred across the Ethernet data networks, as required by O.DATA_PROTECTION.

The cryptographic functions meet the standards required by FIPS 140-2 [15].

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.

O.FLOW FDP_IFC.1, FDP_IFF.1, FMT_MSA.1/ Information Flow Control and FMT_MSA.3/Information Access Control provide the capability for authorised users to control traffic flow between subjects using the Ethernet MAC address or VLAN ID in a manner required by O.FLOW.

O.KEY_MANAGEMENT FCS_CKM.1/AES, RSA, ECDSA, FCS_CKM.2/RSA, AES, ECDSA, DH, ECDH and FCS_CKM.4/SMK, PK, AES provide the capability for generating, distributing and destroying cryptographic keys as required to provide means for exchanging keys with an authorised TOE as required by O.KEY_MANAGEMENT.

FCS_COP.1/RSA_enc and FCS_COP.1/ECDSA_enc provide RSA encryption of KEKs or ECDH generation of DEKs.

FCS_COP.1/AES_Key provides AES encryption of the encryptor RSA and ECDSA keys.

These cryptographic functions meet the standards required by FIPS 140-2 [15].

O.REMOTE_MANAGEMENT FCS_COP.1/AES_Data provides the capability for encryption methods for management data over the network.

FIA_UAU.5 provides the capability to authenticate a user remotely.

O.ROLE_MANAGEMENT FTA_SSL.3 provides additional protection by automatically terminating management sessions after a period of user inactivity.

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.

FIA_UAU.2 and FIA_UID.2 provide the capability for identifying and authenticating all users in a manner required by O.ROLE_MANAGEMENT.

FIA_UAU.5 provides the capability to identify and authenticate all users localy or remotely.

FIA_AFL.1 provides additional protection by limiting the number of unsuccessful authentication attempts before imposing a timeout on that user account.

FMT_SMR.1 specifies the four possible roles administrator, supervisor, operator and upgrader.

FMT_SMR.1 associates a human with one role.

In combination, these SFRs restrict the human's access to only those TSF attributes, data and operations explicitly allowed by the associated role.

5.4.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.AUDIT	FAU_GEN.1, FAU_SAR.1, FPT_STM.1	Section 5.3.1
O.CERT_MANAGEMENT	FCS_COP.1/RSA_enc, FCS_COP.1/SHA, FCS_COP.1/RSA_sign, FDP_DAU.1, FTP_ITC.1, FCS_COP.1/ECDSA_enc, FCS_COP.1/ECDSA_sign, FCS_COP.1/AES_Key	Section 5.3.1
O.DATA_PROTECTION	FCS_COP.1/AES_Data, FDP_UCT.1	Section 5.3.1
O.SECURE_STATE	FPT_FLS.1, FPT_TST.1	Section 5.3.1
O.FLOW	FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3	Section 5.3.1
O.KEY_MANAGEMENT	FCS_COP.1/RSA_enc, FCS_CKM.1/AES, FCS_CKM.1/RSA, FCS_CKM.1/ECDSA, FCS_CKM.2/RSA, FCS_CKM.2/AES, FCS_CKM.2/ECDSA, FCS_CKM.4/SMK, FCS_COP.1/ECDSA_enc, FCS_CKM.4/PK, FCS_CKM.4/AES, FCS_CKM.2/DH, FCS_CKM.2/ECDH, FCS_COP.1/AES_Key.	Section 5.3.1
O.REMOTE_MANAGEMENT	FCS_COP.1/AES_Data, FIA_UAU.5	Section 5.3.1
O.ROLE_MANAGEMENT	FTA_SSL.3, FMT_MTD.1, FMT_SMF.1, FIA_UAU.2, FIA_AFL.1, FMT_SMR.1, FIA_UAU.5, FIA_UID.2	Section 5.3.1

Table 12 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_GEN.1	O.AUDIT
FAU_SAR.1	O.AUDIT
FIA_AFL.1	O.ROLE_MANAGEMENT
FIA_UAU.2	O.ROLE_MANAGEMENT
FIA_UAU.5	O.REMOTE_MANAGEMENT, O.ROLE_MANAGEMENT
FIA_UID.2	O.ROLE_MANAGEMENT
FDP_DAU.1	O.CERT_MANAGEMENT
FDP_IFC.1	O.FLOW
FDP_IFF.1	O.FLOW
FDP_UCT.1	O.DATA_PROTECTION

FCS_CKM.1/AES	O.KEY_MANAGEMENT
FCS_CKM.1/RSA	O.KEY_MANAGEMENT
FCS_CKM.1/ECDSA	O.KEY_MANAGEMENT
FCS_CKM.2/RSA	O.KEY_MANAGEMENT
FCS_CKM.2/AES	O.KEY_MANAGEMENT
FCS_CKM.2/ECDSA	O.KEY_MANAGEMENT
FCS_CKM.4/SMK	O.KEY_MANAGEMENT
FCS_CKM.4/PK	O.KEY_MANAGEMENT
FCS_CKM.4/AES	O.KEY_MANAGEMENT
FCS_CKM.2/DH	O.KEY_MANAGEMENT
FCS_CKM.2/ECDH	O.KEY_MANAGEMENT
FCS_COP.1/AES_Key	O.CERT_MANAGEMENT, O.KEY_MANAGEMENT
FCS_COP.1/AES_Data	O.DATA_PROTECTION, O.REMOTE_MANAGEMENT
FCS_COP.1/RSA_enc	O.CERT_MANAGEMENT, O.KEY_MANAGEMENT
FCS_COP.1/ECDSA_enc	O.CERT_MANAGEMENT, O.KEY_MANAGEMENT
FCS_COP.1/SHA	O.CERT_MANAGEMENT
FCS_COP.1/RSA_sign	O.CERT_MANAGEMENT
FCS_COP.1/ECDSA_sign	O.CERT_MANAGEMENT
FMT_MSA.1	O.FLOW
FMT_MSA.3	O.FLOW
FMT_MTD.1	O.ROLE_MANAGEMENT
FMT_SMF.1	O.ROLE_MANAGEMENT
FMT_SMR.1	O.ROLE_MANAGEMENT
FPT_FLS.1	O.SECURE_STATE
FPT_STM.1	O.AUDIT
FPT_TST.1	O.SECURE_STATE
FTA_SSL.3	O.ROLE_MANAGEMENT
FTP_ITC.1	O.CERT_MANAGEMENT

Table 13 SFRs and Security Objectives

5.4.3 Dependencies

5.4.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_GEN.1	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.2
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2
FIA_UAU.5	No Dependencies	
FIA_UID.2	No Dependencies	
FDP_DAU.1	No Dependencies	
FDP_IFC.1	(FDP_IFF.1)	FDP_IFF.1
FDP_IFF.1	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1, FMT_MSA.3
FDP_UCT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1, FTP_ITC.1
FMT_MSA.1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FPT_FLS.1	No Dependencies	
FPT_STM.1	No Dependencies	
FPT_TST.1	No Dependencies	
FTA_SSL.3	No Dependencies	
FTP_ITC.1	No Dependencies	
FCS_CKM.1/AES	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4/SMK, FCS_COP.1/AES_Key FCS_COP.1/AES_Data
FCS_CKM.1/RSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.2/RSA, FCS_CKM.4/SMK
FCS_CKM.1/ECDSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.2/ECDSA, FCS_CKM.4/SMK
FCS_CKM.2/RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4/SMK
FCS_CKM.2/AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AES, FCS_CKM.4/AES

FCS_CKM.2/ECDSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ECDSA, FCS_CKM.4/SMK
FCS_CKM.4/SMK	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	
FCS_CKM.4/PK	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/RSA, FCS_CKM.1/ECDSA
FCS_CKM.4/AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/AES
FCS_CKM.2/DH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AES, FCS_CKM.4/AES
FCS_CKM.2/ECDH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ECDSA, FCS_CKM.4/PK
FCS_COP.1/AES_Key	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SMK
FCS_COP.1/AES_Data	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/AES, FCS_CKM.4/SMK
FCS_COP.1/RSA_enc	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4/SMK
FCS_COP.1/ECDSA_enc	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ECDSA, FCS_CKM.4/SMK
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/RSA_sign	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA, FCS_CKM.4/SMK
FCS_COP.1/ECDSA_sign	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/ECDSA, FCS_CKM.4/SMK

Table 14. SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. This is a hash function, and thus there is no need for key generation.

The dependency FCS_CKM.4 of FCS_COP.1/SHA is discarded. This is a hash function, and thus there is no need for key destruction.

5.4.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ALC_FLR.3	No Dependencies	
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3

ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.1, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.1	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 15. SARs Dependencies

5.4.4 Rationale for the Security Assurance Requirements

EAL4 assurance level has been chosen because the TOE is intended to be used to protect sensitive information transmitted between critical networks in both the civil and the military sectors.

5.4.5 ALC_FLR.3 Systematic flaw remediation

Senetas has chosen to augment EAL4 by adding the assurance component ALC_FLR.3 to assure that TOE users will know how to report security flaws, and that Senetas will act appropriately to address security flaws.

6. TOE Summary Specification

6.1 TOE Summary Specification

SF.AUDIT

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. It also contains a Real Time Clock (RTC) from which a timestamp is obtained for each audit record.

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.

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.

SF.CERTIFICATE_MANAGEMENT

The TOE shall manage all necessary tasks to support X.509 certificate based authentication. These tasks consist of:

- Generating and installing signed X.509 certificates into the encryptor
- Authenticating received X.509 certificates using installed trusted CA root certificates

Operations related to generating X.509 certificates require the use of the RSA or ECDSA algorithms to generate the private and public key pair, while signing operations are performed using the RSA or ECDSA signature algorithms.

Before installing X.509 certificates for the first time, the default user credentials are updated using a process of RSA asymmetric key exchange. This process is referred to as activation of the encryptor. 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 CN series encryptor or on the Command Line Interface 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.

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.

Once activated, CM7 can be used to request any number of CSRs (Certificate Signing Requests) from the encryptor. When acting as the CA, CM7 may sign these CSRs directly and return the X.509 certificate(s) to the encryptor. Alternatively, CM7 can save the CSRs for signing by an external CA. Once signed, the resulting X.509 certificate(s) are installed using CM7. The Encryptor uses these certificates to establish trusted communications channels between itself and other Encryptors (remote trusted IT products). Both encryptors must have a valid X.509 certificate, in which the root trust anchor can be validated (trusted CA), to protect the confidentiality and integrity of transmitted information and these are

logically distinct from other channels. X.509 V3 certificates use the SHA-256 hashing algorithm.

SF.DATA_EXCHANGE

The TOE encrypts the payload on the basis of the address in the ethernet frame and whether the CI entry requires encryption of traffic on that address.

If encryption is required, the encryptor performs hardware based 128 or 256 bit AES encryption in CFB, counter (CTR) mode, or GCM on the Ethernet frame payload and a user configurable portion of the header.

SF.IDENTIFICATION

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.

All user passwords must have a minimum length of 14 characters.

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.

Alternatively the CLI can be accessed remotely via SSH (when configured). 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.

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.

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

SF.KEY_MANAGEMENT

The TOE shall manage all the necessary keys and mechanisms to support its cryptographic operations, namely:

- Generating public/private key pairs.

- Generating and securely transferring KEKs between encryptors. Keys are distributed between encryptors using RSA-OAEP public key cryptography in accordance with NIST SP800-56B. Alternatively, ECDSA/ECDH ephemeral key agreement is used to distribute cryptographic keys in accordance with NIST SP800-56A.
- Updating DEKs used for AES encryption between encryptors. AES DEKs are periodically updated according to local security policy requirements set by Administrators or Supervisors. New DEKs are exchanged AES encrypted using the current KEK and authenticated using HMAC.
- Generating a shared secret via a Diffie-Hellman Key-Agreement for SNMPv3 management.
- Protecting user passwords used for user authentication. During user account setup on an encryptor, the user's password is encrypted using the encryptor's System Master Key. The encryption is performed using AES.
- KEKs and DEKs held in volatile memory (RAM) are erased on loss of power.

SF.INFORMATION_FLOW_CONTROL

The TOE shall control the flow of Ethernet frames received on the private network interface and on the public network interface from external hosts on the basis of the MAC address or VLAN ID in the Ethernet frame[12]. In doing so, the TOE shall take one of the following four possible actions, encrypt the payload, decrypt the payload, pass the payload unchanged, or discard the payload.

The TOE determines the appropriate action to take on any given frame by examining the list of entries in the CI table. By default, for a given address that is not listed in the CI table the frame is discarded.

The CI table initially contains no entries. Hence all received information on the local and network ports is discarded. The Administrator and Supervisor roles can specify alternative values in the CI table to override the default values.

SF.ROLE_BASED_ACCESS

The TOE can be accessed and managed using SNMPv3 packets received on the Ethernet management port and network interface or via the console management port interface. The encryptor's USB port can be used to upgrade firmware.

Users will be allowed access to the TOE when a valid user ID and password are provided. Additionally, any packets or sessions (i.e. SNMPv3) must be properly authenticated for access to be obtained. SNMPv3 uses a privacy key that is associated with the user id to optionally encrypt/decrypt the packets. If any of these conditions are not met, then access will be denied. The TOE defines four roles for accessing the TSFs:

- 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[13].
- 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.

[12] The iSID connection mode is out of the scope of the certification. To be in a certified configuration, the iSID mode should not be used.

[13] FTP is also supported but must not be used (as stated in AGD_OPE [10]).

- Operators: can query the CI and User Account tables only, and view the audit log.
- Upgraders: can remotely upgrade the firmware via either USB, SFTP or FTPS[13], query the CI and User Account tables and view the audit log.

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.

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

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

SF.SELF_PROTECT

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.

6.2 SFRs and TSS

6.2.1 SFRs and TSS - Rationale

6.2.1.1 TOE Summary Specification

SF.AUDIT The encryptor is able to generate an audit record for each of the auditable events listed in FAU_GEN.1. The encryptor has a Real Time Clock (RTC) from which a timestamp is obtained for each audit record (FPT_STM.1).

The data is presented in a human readable format, with CM7 and the console mode presenting the data as a scrolled list of audit text (FAU_SAR.1).

SF.CERTIFICATE_MANAGEMENT Operations related to the generation of X.509 certificates require the use of the RSA or ECDSA algorithms to generate the private and public key pair (FCS_COP.1/RSA_enc and FCS_COP.1/ECDSA_enc).

X.509 certificate signing operations are done using the RSA or ECDSA (FCS_COP.1/RSA_sign and FCS_COP.1/ECDSA_sign) signature algorithms.

For activation, the encryptor hashes the certificate using SHA-256 (FCS_COP.1/SHA) to create a validation code (FDP_DAU.1). The validation code is then displayed on the front panel of the CN series encryptor or on the Command Line Interface where no front panel display exists (FDP_DAU.1).

Encryptors must have a valid X.509 certificate, in which the root trust anchor can be validated (trusted CA), to protect the confidentiality and integrity of transmitted information and these are logically distinct from other channels (FTP_ITC.1). X.509 V3 certificates use the SHA-256 hashing algorithm (FCS_COP.1/SHA).

Certificates private keys are stored encrypted using AES in the TOE non volatile memory (FCS_COP.1/AES_Key).

SF.DATA_EXCHANGE If encryption is required, the encryptor performs hardware-based 128 or 256 bit AES encryption in CFB, counter (CTR), or GCM mode (FCS_COP.1/AES_DATA) on the Ethernet frame payload and a user configurable portion of the header (FDP_UCT.1).

SF.IDENTIFICATION To modify and view any of the security attributes of the TOE, authorised users must identify (FIA_UID.2) and authenticate (FIA_UAU.2) via one of two mechanisms depending on whether they are using the SNMPv3 functionality or the console management functionality.

A local or remote password-based authentication mechanism may be used (FIA_UAU.5, FCS_COP.1/SHA). The authentication for remote CLI access and download of firmware updates (via SFTP or FTPS) relies on ECDSA (FCS_COP.1/ECDSA_sign, FCS_COP.1/SHA).

After three consecutive unsuccessful logon attempts, the user account will be disabled for three minutes (FIA_AFL.1).

After a period of 10 minutes of inactivity, the console user session will be automatically terminated (FTA_SSL.3).

SF.KEY_MANAGEMENT The TOE manages several keys:

- Generation of keys: RSA (FCS_CKM.1/RSA) or ECDSA (FCS_CKM.1/ECDSA), KEK (FCS_CKM.1/AES) and Master Key (FCS_CKM.1/AES)
- Transfer of keys: RSA (FCS_COP.1/RSA_enc) or ECDSA (FCS_COP.1/ECDSA_enc), AES (FCS_CKM.2/AES, FCS_COP.1/AES_Data), DH or ECDH (FCS_CKM.2/DH, FCS_CKM.2/ECDH, FCS_CKM.2/RSA and FCS_CKM.2/ECDSA)
- Destruction of keys (FCS_CKM.4)

The encryption is performed using AES (FCS_COP.1/AES_Key)

SF.INFORMATION_FLOW_CONTROL The control the flow of Ethernet frames received on the private network interface and on the public network interface from external hosts is ensured by FDP_IFC.1 and FDP_IFF.1.

FMT_MSA.1 and FMT_MSA.3 ensure that the Administrator and Supervisor roles can change MAC addresses or VLAN IDs for Ethernet frames and specify alternative values in the CI table to override the default values.

SF.ROLE_BASED_ACCESS The TOE defines four roles for accessing the TSFs (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3). Once successfully authenticated, the user is granted access to the operations/actions allowed by his role (FCS_COP.1/ECDSA_sign, FCS_COP.1/SHA). In particular, only administrators and upgraders can perform firmware upgrades. The TOE also checks the authenticity and integrity of firmware update images before performing firmware upgrade (FCS_COP.1/RSA_sign).

SF.SELF_PROTECT The self-test execution during TOE start-up is ensured by FPT_TST.1. The preservation of the TOE secure state is ensured by FPT_FLS.1

6.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_GEN.1	SF.AUDIT
FAU_SAR.1	SF.AUDIT
FIA_AFL.1	SF.IDENTIFICATION
FIA_UAU.2	SF.IDENTIFICATION
FIA_UAU.5	SF.IDENTIFICATION
FIA_UID.2	SF.IDENTIFICATION
FDP_DAU.1	SF.CERTIFICATE_MANAGEMENT
FDP_IFC.1	SF.INFORMATION_FLOW_CONTROL
FDP_IFF.1	SF.INFORMATION_FLOW_CONTROL
FDP_UCT.1	SF.DATA_EXCHANGE
FCS_CKM.1/AES	SF.KEY_MANAGEMENT
FCS_CKM.1/RSA	SF.KEY_MANAGEMENT
FCS_CKM.1/ECDSA	SF.KEY_MANAGEMENT
FCS_CKM.2/RSA	SF.KEY_MANAGEMENT
FCS_CKM.2/AES	SF.KEY_MANAGEMENT
FCS_CKM.2/ECDSA	SF.KEY_MANAGEMENT
FCS_CKM.4/SMK	SF.KEY_MANAGEMENT
FCS_CKM.4/PK	SF.KEY_MANAGEMENT
FCS_CKM.4/AES	SF.KEY_MANAGEMENT
FCS_CKM.2/DH	SF.KEY_MANAGEMENT
FCS_CKM.2/ECDH	SF.KEY_MANAGEMENT
FCS_COP.1/AES_Key	SF.KEY_MANAGEMENT, SF.CERTIFICATE_MANAGEMENT
FCS_COP.1/AES_Data	SF.DATA_EXCHANGE
FCS_COP.1/RSA_enc	SF.CERTIFICATE_MANAGEMENT
FCS_COP.1/ECDSA_enc	SF.CERTIFICATE_MANAGEMENT
FCS_COP.1/SHA	SF.CERTIFICATE_MANAGEMENT, SF.IDENTIFICATION, SF.ROLE_BASED_ACCESS
FCS_COP.1/RSA_sign	SF.CERTIFICATE_MANAGEMENT, SF.ROLE_BASED_ACCESS
FCS_COP.1/ECDSA_sign	SF.CERTIFICATE_MANAGEMENT, SF.IDENTIFICATION, SF.ROLE_BASED_ACCESS
FMT_MSA.1	SF.ROLE_BASED_ACCESS, SF.INFORMATION_FLOW_CONTROL
FMT_MSA.3	SF.INFORMATION_FLOW_CONTROL, SF.ROLE_BASED_ACCESS
FMT_MTD.1	SF.ROLE_BASED_ACCESS
FMT_SMF.1	SF.ROLE_BASED_ACCESS
FMT_SMR.1	SF.ROLE_BASED_ACCESS
FPT_FLS.1	SF.SELF_PROTECT
FPT_STM.1	SF.AUDIT
FPT_TST.1	SF.SELF_PROTECT
FTA_SSL.3	SF.IDENTIFICATION
FTP_ITC.1	SF.CERTIFICATE_MANAGEMENT

Table 16. SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.AUDIT	FAU_GEN.1, FAU_SAR.1, FPT_STM.1
SF.CERTIFICATE_MANAGEMENT	FDP_DAU.1, FTP_ITC.1, FCS_COP.1/RSA_enc, FCS_COP.1/ECDSA_enc, FCS_COP.1/SHA, FCS_COP.1/RSA_sign, FCS_COP.1/ECDSA_sign, FCS_COP.1/AES_Key
SF.DATA_EXCHANGE	FDP_UCT.1, FCS_COP.1/AES_Data
SF.IDENTIFICATION	FIA_AFL.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FCS_COP.1/SHA, FCS_COP.1/ECDSA_sign
SF.KEY_MANAGEMENT	FCS_CKM.1/AES, FCS_CKM.1/RSA, FCS_CKM.1/ECDSA, FCS_CKM.2/RSA, FCS_CKM.2/AES, FCS_CKM.2/ECDSA, FCS_CKM.4/SMK, FCS_CKM.4/PK, FCS_CKM.4/AES, FCS_CKM.2/DH, FCS_CKM.2/ECDH, FCS_COP.1/AES_Key
SF.INFORMATION_FLOW_CONTROL	FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3
SF.ROLE_BASED_ACCESS	FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3, FCS_COP.1/SHA, FCS_COP.1/ECDSA_sign, FCS_COP.1/RSA_sign
SF.SELF_PROTECT	FPT_FLS.1, FPT_TST.1

Table 17. TSS and SFRs - Coverage

7. Notice

7.1 Revisions

Modification	Comment
0.1	First draft version
0.2	Update following Senetas review
0.3	Update of interfaces and removal of optical type interface
0.4	Remove CM7 software from the TOE, Add identification of all products of the family
0.5	Update of software version and its related information
0.6	Minor modifications (typos and removal of irrelevant application notes)
1.0	Minor updates following proofreading
1.1	Add AES GCM mode for CN9100 and CN9120 encryptors
1.2	Update following Intermediate Technical Report, ASE_v1.0 [OUT.001, OUT.002]
1.3	Update following the new Intermediate Technical Report, ASE_v2.0 [OUT.016, OUT.008]
1.4	Update of software version and Section 6.2 following exchanges with the evaluators
1.5	Addition of the A.FTP_Server assumption and update of the security objectives section accordingly
1.6	Changes to address Oppida review comments
1.7	Remove TACACS+ from scope of certification due to non-allowed algorithms
1.8	Add FIA_UAU.5.2
1.9	Changes to address ANSSI comments
2.0	Published version

Table 18. Revision

8. ANNEX

8.1 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	TOE Security Policy

8.2 Glossary

AAA	Authentication, Authorization and Accounting
CA	Certification Authority
CC	Common Criteria
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
FIPS PUB	Federal Information Processing Standard Publication
Gbps	Gigabits per second
IP	Internet Protocol
MAC	Media Access Control
Mbps	Megabits per second
OSP	Organisational Security Policy
RFC	Request for Comment
RSA	Rivest Shamir Adleman Public Key Algorithm
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMK	System master key
SNMPv3	Simple Network Management Protocol Version 3
SSH	Secure Shell
TACACS+	Terminal Access Control Access Control Server
TSS	TOE Summary Specification

X.509	Digital Certificate Standard
CI	Connection Identifier representing established security association
Tunnel	Equivalent to CI
KEK	Key used to encrypt DEK
DEK	Key used to encrypt defined segments of user data traffic
CM7	Senetas PC based remote Management Application
Activation	Process of replacing default user credentials using RSA X.509 fingerprint
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
OAEP	Optimal Asymmetric Encryption Padding
HMAC	Hash-based Message Authentication Code
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
SFTP	SSH File Transfer Protocol

8.3 References

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001.

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002.

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004.

[5] *Australian Government Information and Communications Technology Security Manual (ISM)* previously known as ACSI 33, 2017.

[6] Senetas Ltd., SME Protocol Specification, TBD.

[7] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FIPS PUB 180-1 Secure Hash Algorithm.*

[8] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FIPS PUB 186-2 Digital Signature Standard.*

[9] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FIPS PUB 197 Advanced Encryption Standard.*

[10] National Institute of Standards and Technology, *NIST Special Publication SP800-38A Recommendation for Block Cipher Modes of Operation.*

[11] RSA Laboratories, *PKCS #1 v2.0 RSA Cryptography Standard,* July 14, 1998.

[12] RSA Laboratories, *PKCS 12 v1.0: Personal Information Exchange Syntax*, RSA Laboratories June 24, 1999.

[10] The Internet Engineering Task Force, *RFC 2459 Internet X.509 Public Key Infrastructure*, January 1999.

[11] The Internet Engineering Task Force, *RFC 2574 User-based Security Model for version 3 of the Simple Network Management Protocol*, April 1999.

[12] RSA Laboratories, *PKCS #3 v1.4 Diffie-Hellman Key-Agreement Standard*, November 1993.

[13] National Institute of Standards and Technology, *FIPS PUB 186-4 Digital Signature Standard.*

[14] National Institute of Standards and Technology, *Special Publication SP800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.*

[15] National Institute of Standards and Technology, *Security Requirements for Cryptographic*

Modules, FIPS PUB 140-2, November 2001.
[16] Senetas Ltd. and Gemalto, *Safenet Ethernet Encryptor CN6010 User Guide (Windows Operating System),* Release 05, July 2020, CN6010_ETH_CM7.
[17] Senetas Ltd., *Senetas CN Series Encryptor -Operational User Guidance (AGD_OPE.1),* v1.8, May 2021.
[18] Senetas Ltd., *Senetas CN Series Encryptor - Preparative Procedures (AGD_PRE.1),* v1.8, May 2021.

9. Index