

Security Target for

Senetas CN-Series Encryptor-Range
&
Senetas CM7 Management Application

Compliant to the Common Criteria

Copyright ©2016 Senetas Corporation Ltd.

ABN 31 080 481 947

The information contained in this document remains the property of Senetas Corporation Ltd. It is supplied in confidence with the understanding that it will not be used or disclosed for any purpose other than the Common Criteria evaluation.

All rights are reserved by Senetas Corporation Ltd.

No part may be photocopied, stored in electronic form, reproduced or translated to another language without the prior written consent of Senetas Corporation Ltd.

Version

Version 0.2	29 Mar 2016	Initial Security target draft for software version 2.7.1 submission
Version 1.0	13 May 2016	Final version for submission
Version 1.1	15 Aug 2016	Updated to address EOR 001 v1.0
Version 1.2	13 Dec 2016	Updated to address EOR 001 v2.0
Version 1.3	14 Feb 2017	Updated to address comments from ASD

Table of Contents

1	Introduction.....	6
1.1	OVERVIEW	6
1.2	COMMON CRITERIA CONFORMANCE.....	6
1.3	PROTECTION PROFILE CLAIM.....	6
1.4	IDENTIFICATION.....	6
1.4.1	<i>Common Criteria Identification</i>	6
1.4.2	<i>Security Target Identification</i>	6
1.4.3	<i>TOE Identification</i>	6
1.4.4	<i>CN Series Models</i>	7
1.5	REFERENCES.....	7
1.6	GLOSSARY OF KEY TERMS	9
2	TOE Description	10
2.1	OVERVIEW	10
	SECURITY FEATURES	12
2.1.1	<i>Ethernet Processing</i>	12
2.1.2	<i>Fibre Channel Processing</i>	13
2.2	SECURE MANAGEMENT	14
2.2.1	<i>Activation</i>	14
2.2.2	<i>Certification Authority</i>	14
2.2.3	<i>Local Management</i>	14
2.2.4	<i>Remote Management using CLI over SSH</i>	14
2.2.5	<i>Remote Management using SNMPv3</i>	14
2.2.6	<i>TACACS+</i>	15
3	TOE Security Environment	15
3.1	ASSUMPTIONS.....	15
3.2	THREATS.....	17
3.3	ORGANISATIONAL SECURITY POLICIES.....	19
4	Security Objectives	20
4.1	TOE SECURITY OBJECTIVES.....	20
4.2	ENVIRONMENTAL SECURITY OBJECTIVES.....	22
5	IT Security Requirements	24
5.1.1	<i>Security Audit (FAU)</i>	24
5.1.2	<i>Cryptographic Support (FCS)</i>	25
5.1.3	<i>User Data Protection (FDP)</i>	28
5.1.4	<i>Identification and Authentication (FIA)</i>	30
5.1.5	<i>Security Management (FMT)</i>	31

5.1.6	<i>Protection of the TSF (FPT)</i>	33
5.1.7	<i>TOE Access (FTA)</i>	34
5.1.8	<i>Trusted Path/Channels (FTP)</i>	34
5.2	TOE SECURITY ASSURANCE REQUIREMENTS	35
5.3	SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT	35
6	TOE Summary Specification	36
6.1	TOE IT SECURITY FUNCTIONS	36
7	Rationale	45
7.1	SECURITY OBJECTIVES RATIONALE	45
7.1.1	<i>Mapping of Threats, OSPs and Assumptions to Security Objectives</i>	45
7.1.2	<i>Informal argument of adequacy and correctness of mapping</i>	46
7.2	SECURITY REQUIREMENTS RATIONALE	53
7.2.1	<i>Mapping of Security Functional Requirements to Security Objectives</i>	53
7.2.2	<i>Informal Argument of Sufficiency</i>	55
7.2.3	<i>Rationale for EAL2+ ALC_FLR.2 Assurance level</i>	58

List of Tables

Table 1 – CN Series & CM7 Application Software Versions	7
Table 2 – CN Series Model Numbers	7
Table 3 – TOE Security Environmental Assumptions	17
Table 4 – TOE Security Environmental Threats.....	18
Table 5 – TOE Security Environment Organisational Security Policies	19
Table 6 – TOE Security Objectives	21
Table 7 – Environmental Security Objectives	23
Table 8 – TOE IT Security Functions.....	44
Table 9 – Mapping of Threats, OSPs and Assumptions to Security Objectives	45
Table 10 – Informal argument of assumptions	46
Table 11 – Informal argument of threats	51
Table 12 – Informal argument of policies.....	52
Table 13 – Mapping of Security Functional Requirements to Security Objectives	54
Table 14 – Informal Argument of Sufficiency.....	58

List of Figures

Figure 1 – Encryption data flow diagram	10
Figure 2 – Ethernet Security Solution.....	11
Figure 3 – Fibre Channel Security Solution.....	11

1 Introduction

1.1 Overview

This document provides a complete and consistent statement of the security enforcing functions and mechanisms of the Target of Evaluation (TOE). The TOE consists of:

- CN series encryptor;
- CM7 management application software.

The ST details the TOE security requirements and the countermeasures proposed to address the perceived threats to the assets protected by the TOE.

The CN series encryptors are high-speed, standards based multi-protocol encryptors specifically designed to secure voice, data and video information transmitted over Ethernet and Fibre Channel data networks at data rates up to 10 Gigabits per second. It also provides access control facilities using access rules for each defined Ethernet or Fibre Channel connection.

The CM7 management application is a Graphical User Interface (GUI) software package that runs on Windows platforms. It can act as a Certification Authority (CA) for signing X.509 certificates, or alternatively supports the use of external CA PKI environments. It provides secure remote installation of X.509 certificates into the Senetas encryptors using SNMPv3, and is also used to securely manage the encryptors.

1.2 Common Criteria Conformance

The TOE is Part 2 Conformant and Part 3 Conformant to the Common Criteria. The TOE is conformant to Evaluation Assurance Level EAL2+ ALC_FLR.2.

1.3 Protection Profile Claim

The TOE has not been designed to comply with any known Protection Profile and accordingly no claim is made.

1.4 Identification

This section provides information needed to identify and control this Security Target and its Target of Evaluation.

1.4.1 Common Criteria Identification

Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.4.2 Security Target Identification

ST Title: Senetas Encryptor Security Target

ST Version: 1.1

ST Issue Date: August 2016

1.4.3 TOE Identification

The following encryptor and remote management application Software versions apply to this evaluation:

Description	Version	Applicable CN Series Model Numbers
CN Series Application Software	2.7.1	Applies to all CN units
CM7 Management Application Software	7.5.1	Applies to all units

Table 1 – CN Series & CM7 Application Software Versions

Senetas CN series Model numbers applicable to this evaluation are listed in Table 2; note the two main variants with optional power supply configurations.

1.4.4 CN Series Models

ID	Description
A6040B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC UNIT
A6041B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) DC UNIT
A6042B	CN6040 1G ETHERNET + 1/2/4G Fibre Channel (SFP+RJ45) AC/DC UNIT
A6100B	CN6100 10G ETHERNET (XFP) AC UNIT
A6101B	CN6100 10G ETHERNET (XFP) DC UNIT
A6102B	CN6100 10G ETHERNET (XFP) AC/DC UNIT
A6010B	CN6010 1G ETHERNET (SFP+RJ45) AC UNIT
A6011B	CN6010 1G ETHERNET (SFP+RJ45) DC UNIT
A6012B	CN6010 1G ETHERNET (SFP+RJ45) AC/DC UNIT
A4020B	CN4020 1G ETHERNET UNIT
A4010B	CN4010 1G ETHERNET UNIT
A8003-10	CN8000 MULTI-SLOT 1/10G ETHERNET + 1/2/4G Fibre Channel (SFP+) AC UNIT

Table 2 – CN Series Model Numbers

1.5 References

1. Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 4, September 2012
2. Australian Government Information and Communications Technology Security Manual (ISM) previously known as ACSI 33, December 2008
3. ATM Security Specification Version 1.1 af-sec-0100.002 March 2001
4. FIPS PUB 180-1 Secure Hash Algorithm
5. FIPS PUB 186-2 Digital Signature Standard
6. FIPS PUB 197 Advanced Encryption Standard
7. NIST Special Publication SP800-38A Recommendation for Block Cipher Modes of Operation
8. PKCS #1 v2.0 RSA Cryptography Standard, RSA Laboratories July 14, 1998
9. PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories June 24, 1999
10. RFC 2459 Internet X.509 Public Key Infrastructure IETF, January 1999

11. RFC 2574 User-based Security Model for version 3 of the Simple Network Management Protocol, IETF, April 1999
12. PKCS #3 v1.4 Diffie-Hellman Key-Agreement Standard, RSA Laboratories, November 1993
13. FIPS PUB 186-4 Digital Signature Standard
14. NIST Special Publication SP800-56A Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

1.6 Glossary of Key Terms

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
PP	Protection Profile
RFC	Request for Comment
RSA	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
ST	Security Target
TACACS+	Terminal Access Control Access Control Server
TOE	Target of Evaluation
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

2 TOE Description

2.1 Overview

The Senetas CN series encryptors are high-speed, standards based multi-protocol encryptors specifically designed to secure voice, data and video information transmitted over Fibre Channel and Ethernet Networks. They can be deployed within Networks employing data rates up to 10 Gigabits per second and provide support for the AES algorithm. All of the encryptors in the CN series offer a single encryption path per encryptor except for the CN8000 Multi-slot encryptor which supports up to 10 interface/ high speed crypto cards (Slots) per chassis, each independently configurable as 1G or 10G Ethernet or 1, 2, 4G Fibre Channel. The encryptors also provide access control facilities using access rules for each defined Ethernet and Fibre Channel connection.

The Senetas CN Series Ethernet connects to the Local Area Network (LAN) or Wide Area Network (WAN) using 10/100/1000 BaseT RJ45 or Optical Fibre connectors. When operating at full bandwidth, the Ethernet encryptor will not discard any valid Ethernet frames for all modes of operation.

The Senetas CN series Fibre Channel connects to Fibre Channel links to provide traffic encryption over point to point (link) network segments at speeds of 1, 2, and 4 Gbps. Single and Multi Mode Optical Interfaces can be used to provide short and long haul transmission capability. The product has been designed to integrate simply and transparently into existing Fibre Channel network architectures and provides the ability to encrypt Fibre Channel traffic with no packet expansion, and minimal management overhead, allowing full line speed data throughput.

The CN8000 and CN6040 products are user switchable between Fibre Channel and Ethernet encryption modes within the same physical encryptor.

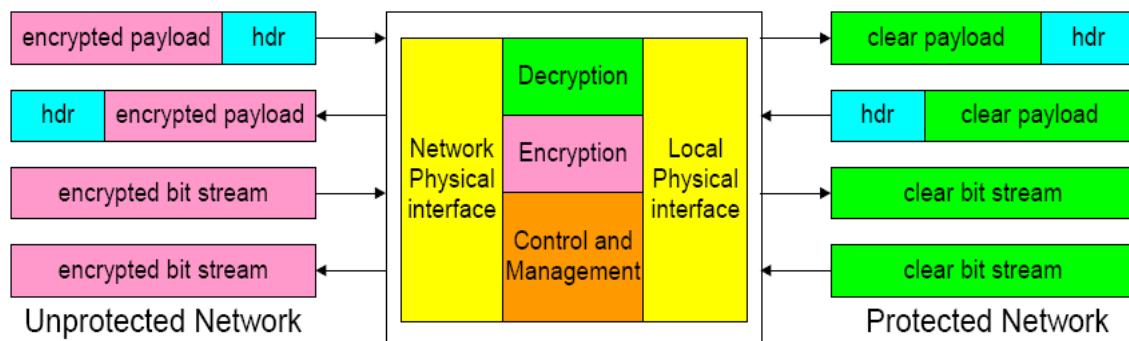


Figure 1 – Encryption data flow diagram

The encryptors provide access control and authentication between secured sites and confidentiality of

transmitted information by cryptographic mechanisms. The encryptors can be added to an existing network with complete transparency to the end user and network equipment. An example installation of a Senetas CN series Ethernet encryptor is shown in Figure 2 and a Fibre Channel encryptor is shown in Figure 3

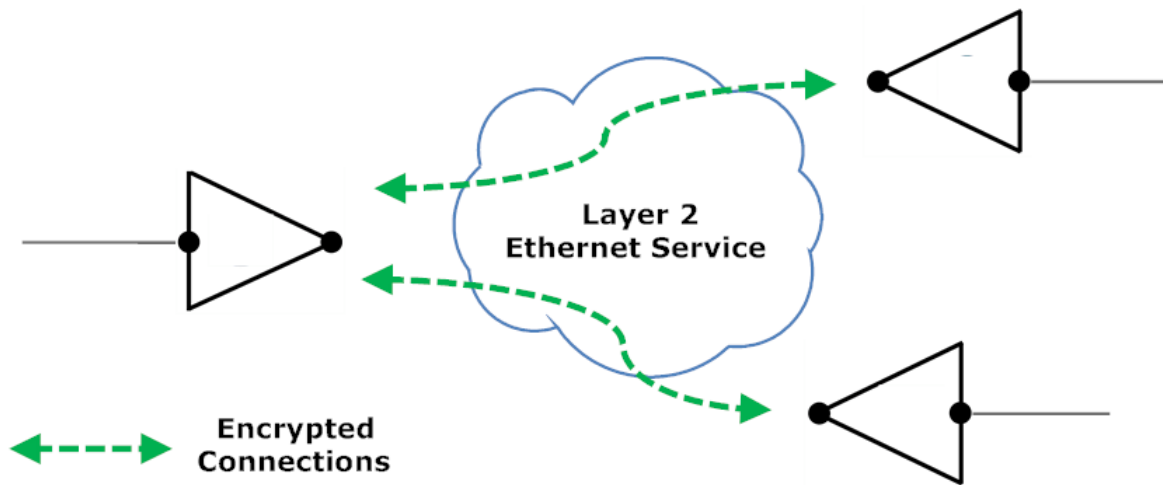


Figure 2 – Ethernet Security Solution

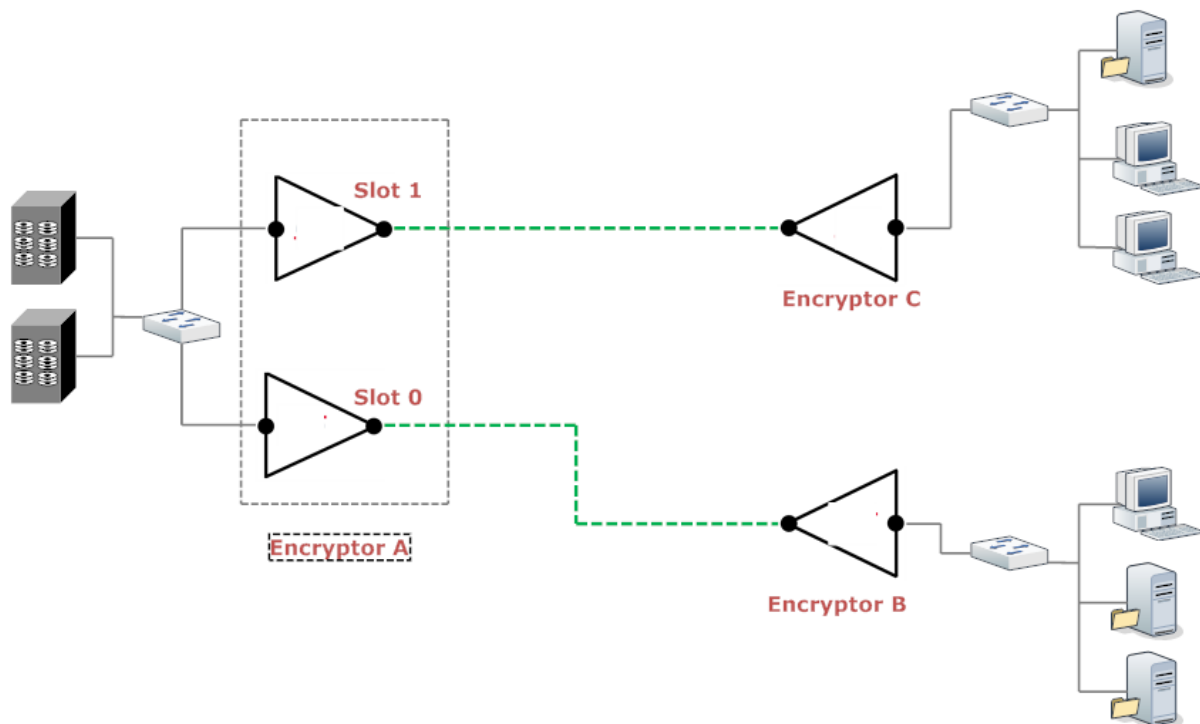


Figure 3 – Fibre Channel Security Solution

The Senetas CN series encryptors can be securely remotely managed by using CM7, an SNMPv3 compliant management station. Remote management sessions connect to the encryptor through the dedicated front panel Ethernet port or logically via network interface. The encryptors can also be managed locally through the RS232 console port supporting a Command Line Interface (CLI). The CLI can also be accessed remotely via

SSH (when configured).

The Senetas series encryptors support different types of user roles with different privileges according to a set of pre-defined roles. The four defined roles are Administrator, Supervisor, Operator and Upgrader. Only the Administrator has unrestricted access to the security features of the encryptor. Only Administrators can install X.509 certificates that are required for the encryptor to commence operation.

The Senetas CN series encryptors provide an audit capability to support the effective management of the security features of the device. The audit capability records all management activity for security relevant events.

Any organisation using the encryptors should ensure that an appropriate operational environment is maintained that satisfies those assumptions listed in section 3 of this Security Target.

Security Features

The TOE provides the following security features for each of the supported protocols.

2.1.1 Ethernet Processing

The encryptors provide confidentiality of the Ethernet frame by encrypting the payload of the frame. The twelve-byte Ethernet frame header is unchanged, which enables switching of the frame through an Ethernet network. The format of the Ethernet frame is shown in Figure 4. With the advent of gigabit Ethernet, jumbo frames of up to 10,000 bytes are also supported.

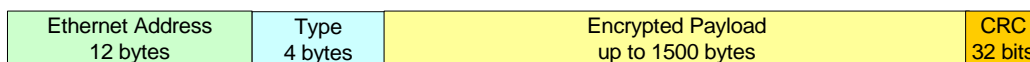


Figure 4 – Ethernet frame format

Public key cryptography (RSA/ECDSA) and X.509 certificates are used to provide a fully automated key management system. Key encrypting keys (KEKs) are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. Data encrypting keys (DEKs) are transferred periodically between encryptors using the associated KEK. Alternatively, ECDSA/ECDH utilises 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 encryptors provide access control by discarding frames if the access rules for that particular virtual circuit are violated. 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.

The following diagram shows the information flow control options involved in processing Ethernet frames:

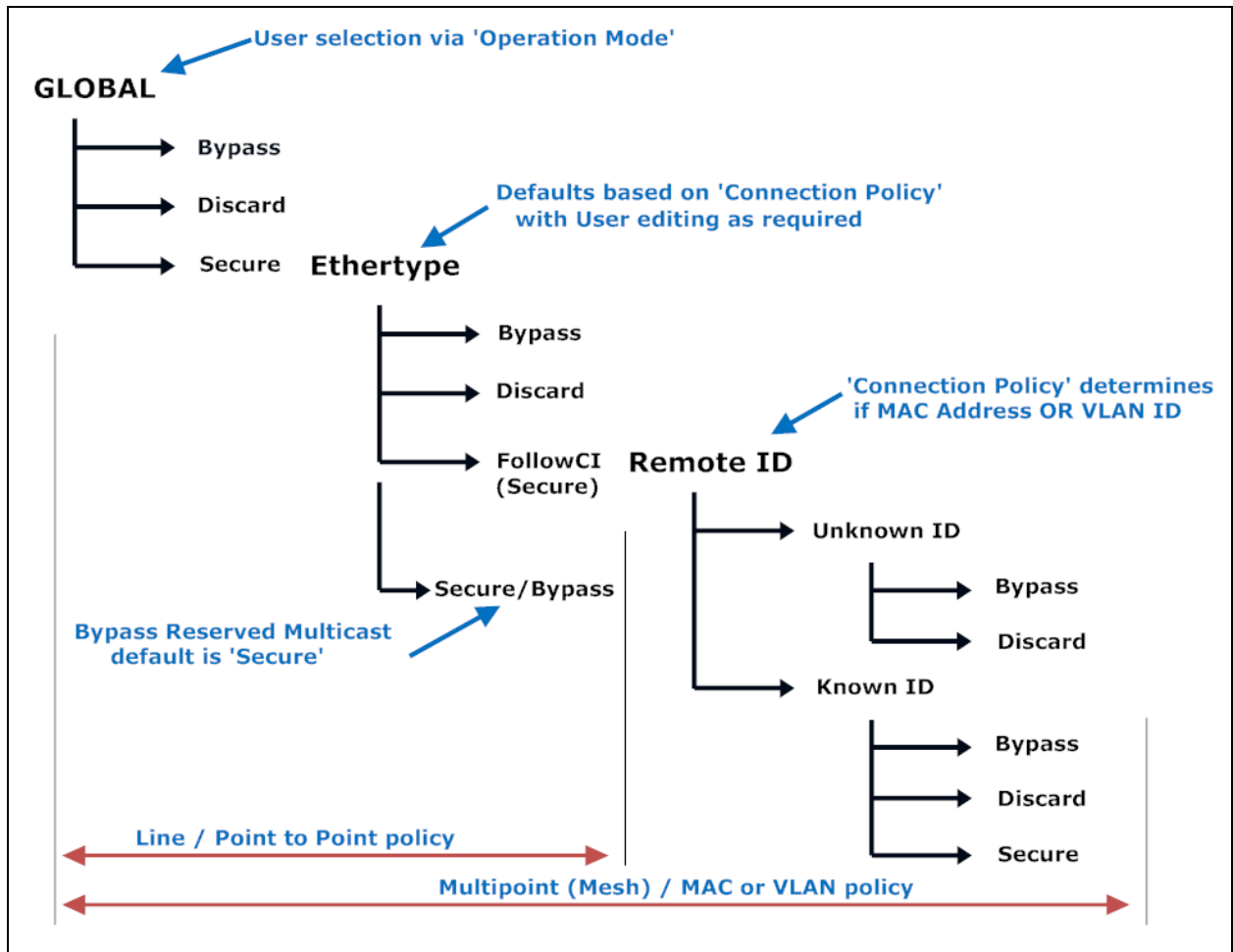


Figure 5 - Information Flow Control: Ethernet frame processing

2.1.2 Fibre Channel Processing

The Senetas CN series provides confidentiality of the Fibre Channel point to point (link) network by encrypting the payload of each Fibre Channel frame (FC-2 layer) and a user selectable portion of the frame header; the format of the Fibre Channel frame is shown in Figure 6.

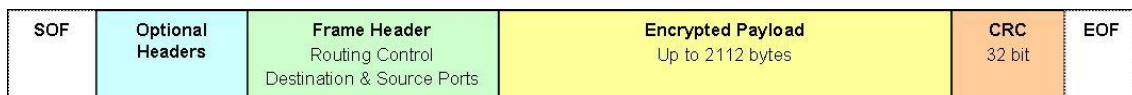


Figure 6– Fibre Channel frame format

RSA public key cryptography and X.509 certificates are used to provide a fully automated key management system. Key encrypting keys (KEKs) are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. Data encrypting keys (DEKs) are transferred periodically between encryptors using the associated KEK.

The Senetas CN series access control for the Fibre Channel session (link) can be set to encrypt, bypass or discard.

2.2 Secure Management

The TOE provides the following secure management features.

2.2.1 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, and validated by the administrator using the front panel display on the Senetas CN series Encryptors. 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.

2.2.2 Certification Authority

Each encryptor must have one or more X.509 certificates installed before the operation of the encryptor can commence. 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 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.

2.2.3 Local Management

Local management is available via an RS232 port supporting a command line interface (CLI). Using a basic terminal emulator (not part of TOE), a user is required to present their user name and authentication password directly to the encryptor before a local management session is allowed.

2.2.4 Remote Management using CLI 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 RSA and ECDSA. RSA Keys must be a minimum of 2048 bits and 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 and 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.

2.2.5 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.

2.2.6 TACACS+

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 disabled by default and cannot be enabled prior to the encryptor being activated. 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 ie: ADMINISTRATOR /SUPERVISOR/OPERATOR/UPGRADER. The remote TACACS+ authentication server is not considered to be within the scope of the evaluated configuration.

3 TOE Security Environment

3.1 Assumptions

The TOE is intended for use by organisations that need to provide confidentiality of information transmitted over Ethernet and Fibre Channel networks and access control to prevent unauthorised connection to the protected network. The following physical, personnel and connectivity assumptions about the operating environment and intended use of the TOE apply.

Assumption	Description
Physical Assumptions	

Assumption	Description
A.CM	<p>The management console, CM7 is assumed to be located within controlled access facilities, which will aid in preventing unauthorised users from attempting to compromise the security functions of the TOE. For example, unauthorised physical access to the CA private key used to sign X.509 certificates.</p> <p>It is assumed that CM7 will be installed on a computer with the following minimum system configuration:</p> <ul style="list-style-type: none"> • Windows NT4.0/2000/XP or higher • 166MHz or higher speed processor • 64MB of memory • Hard disk drive with a minimum of 5MB of available application space • CD drive for installation • SVGA or better display resolution • Mouse or other pointing device • Network adapter card • TCP/IP connectivity
A.LOCATE	<p>It is assumed that the encryptor is located in a secure area at the boundary of the site to be protected. It is required to be in a secure area to ensure that the unit is not physically bypassed.</p>
Personnel Assumptions	
A.ADMIN	<p>It is assumed that one or more administrators, together with any other supervisors or operators, who are 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.</p>
A.AUDIT	<p>It is assumed that appropriate audit 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.</p>
A.PRIVATEKEY	<p>Where CM7 is configured as the Certificate Authority (CA), it is assumed that a password used to protect the private key of the CM7 remote management station is restricted to only Administrators.</p>
Connectivity Assumptions	

Assumption	Description
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. Figure 2 shows how to secure an Ethernet network. Figure 3 shows how to secure a Fibre Channel Link network.

Table 3 – TOE Security Environmental Assumptions

3.2 Threats

This section identifies the threats, which the TOE is designed to counter.

The threat agents against the TOE are defined to have expertise, resources, and motivation that combine to become a basic attack potential for EAL2.

Threat	Description
T.ABUSE	An undetected compromise of information may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.
T.ATTACK	An undetected compromise of information may occur as a result of an attacker (insider or outsider) attempting to perform logical (i.e. non-physical) actions that the individual is not authorised to perform.
T.CAPTURE	An attacker may eavesdrop on or otherwise capture data being transmitted across a public Ethernet or Fibre Channel data network in order to recover information that was to be kept confidential.
T.CONNECT	An attacker (insider or outsider) may attempt to make unauthorised connections to another Ethernet or Fibre Channel data network and transmit information that was to be kept confidential, to another destination.
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.
T.LINK	An attacker may be able to observe multiple uses of services by an entity and, by linking these uses, be able to deduce information, which the entity wishes to be kept confidential.
T.MAL	Data being transmitted across a public Ethernet or Fibre Channel data network may be modified or disclosed to an unauthorised individual or user of the TOE through malfunction of the TOE.

Threat	Description
T.OBSERVE	An attacker could observe the legitimate use of the remote management service by an authorised user when that authorised user wishes their use of that remote management service to be kept confidential.
T.PHYSICAL	Security critical parts of the TOE may be subject to physical attack by an (outside or inside) attacker, which may compromise security.
T.PRIVILEGE	A compromise of information may occur as a result of actions taken by careless, will fully negligent or hostile administrators or other authorised users.

Table 4 – TOE Security Environmental Threats

3.3 Organisational Security Policies

Policy	Description
P.CRYPTO	All encryption services including, confidentiality, authentication, key generation and key management, must conform to standards specified in FIPS PUB 140-2 and ISM.
P.INFOFLOW	<p>Traffic flow is controlled on the basis of the information in the Ethernet frame or Fibre Channel frame and the action specified in the Connection Identifier Table. Any Ethernet frame or Fibre Channel frame for which there is no CI entry is discarded by default. By default, all Ethernet frames and Fibre Channel frames are discarded.</p> <p>The P.INFOFLOW OSP ensures that the correct protective action of bypass, discard or encrypt is applied to any given Ethernet frame or Fibre Channel frame received by the TOE.</p>
P.ROLES	<p>Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users (administrators, supervisors and operators).</p> <p>The P.ROLES OSP ensures that administration of the TOE is performed in accordance with the concept of <i>least privilege</i>.</p>

Table 5 – TOE Security Environment Organisational Security Policies

4 Security Objectives

4.1 TOE Security Objectives

Objective	Description
O.ADMIN	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.
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.CERTGEN	The TOE must provide the means for generating, issuing and managing signed X.509 certificates that conform to standards specified in FIPS PUB 140-2 and ISM. The TOE must use the X.509 certificates to authenticate other encryptors to establish a secure trusted channel between encryptors.
O.ENCRYPT	The TOE must provide the means of protecting the confidentiality of information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB 140-2 and ISM.
O.FAILSAFE	In the event of an error occurring, the TOE will preserve a secure state.
O.INFOFLOW	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 overhead bytes, header or channel information, in accordance with the set of rules defined in the P.INFOFLOW security policy, which includes bypass, discard or encrypt.
O.IDENT	The TOE must uniquely identify all users and authenticate the claimed identity before granting a user access to the TOE management facilities.

O.KEYMAN	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 and ISM.
O.ROLES	The TOE must prevent users from gaining access to and performing operations, on its resources for which their role is not explicitly authorised.
O.TAMPER	The TOE must protect itself and cryptography-related IT assets from unauthorised physical access, modification or use.
O.REMOTEMGT	The TOE must allow secure remote management of the TOE using cryptographic measures that conforms to standards specified in FIPS PUB 140-2 and ISM.

Table 6 – TOE Security Objectives

4.2 Environmental Security Objectives

Objective	Description
O.AUDITLOG	<p>Authorised users of the TOE must ensure that audit facilities are used and managed effectively. In particular:</p> <ol style="list-style-type: none"> a. Appropriate action must be taken to ensure that continued audit logging, e.g. by regular archiving of logs. b. 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.
O.AUTHDATA	<p>Those responsible for the management of the TOE must ensure that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account.</p>
O.CONNECT	<p>Those responsible for the TOE must ensure that no connections are provided to outside systems or users that would undermine IT security.</p>
O.INSTALL	<p>Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.</p>
O.PERSONNEL	<p>Those responsible for the TOE are competent to manage the TOE and can be trusted not to deliberately abuse their privileges so as to undermine security.</p>
O.PHYSICAL	<p>Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack, which might compromise IT security. If a separate Certificate Authority (CA) is used, then those responsible for the TOE must also ensure the CA is protected from physical attacks.</p>
O.ROLEMGT	<p>The administrator responsible for controlling who has access to the unit for configuration and monitoring activities must allocate users roles with the concept of <i>least privilege</i>. There are three roles:</p> <p>Administrator: who has full access rights;</p> <p>Supervisor: who has full access rights except they cannot add, delete or</p>

	<p>modify user accounts, they cannot install X.509 certificates and they cannot upgrade the firmware; and</p> <p>Operator: who can view all available information but cannot delete, add or modify the information</p> <p>Upgrader: who can apply firmware upgrades and can view all available information but cannot delete, add or modify the information</p>
--	---

Table 7 – Environmental Security Objectives

5 IT Security Requirements

The following sections contain the functional components from the Common Criteria Part 2 with the operations completed. The standard Common Criteria text is in regular font; the text inserted is in red italic font.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 – Audit data generation

Hierarchical to: No other components

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 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 ST,
 - FCS_CKM.1 Success and failure of the activity*
 - FCS_CKM.2 Success and failure of the activity*
 - FCS_CKM.4 Success and failure of the activity*
 - FCS_COP.1 Success and failure, and the type of cryptographic operation*
 - FDP_ACF.1 Successful requests to perform an operation on an object covered by the SFP*
 - 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.*
 - FIA_UAU.2 Unsuccessful use of the user authentication mechanism*
 - FIA_UID.2 Unsuccessful use of the user identification mechanism, including the user identity provided*
 - 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*

FTP_ITC.1 Failure of the trusted channel functions
Identification of the initiator and target of failed trusted channel functions

Dependencies: **FPT_STM.1** Reliable time stamps

5.1.1.2 FAU_SAR.1 – Audit review

Hierarchical to: No other components

FAU_SAR.1.1 The TSF shall provide *all authorised users* 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.

Dependencies: **FAU_GEN.1** Audit data generation

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1.A – Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1.A The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *DES, AES* and specified cryptographic key sizes *DES –168 bits, AES – 128 bits, 256 bits* that meet the following: *FIPS PUB 186-2 Digital Signature Standard, Appendix 3.*

Application note: The DES key is used to protect X.509 certificates and user account passwords. AES keys are used in protecting user data during transmission.

Dependencies: **FCS_COP.1** Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

5.1.2.2 FCS_CKM.1.B – Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1.B The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *Diffie-Hellman Key-Agreement with AES keys*, and specified cryptographic key sizes *128 bits* that meet the following: *PKCS #3 and FIPS PUB 186-2 Digital Signature Standard, Appendix 3..*

Dependencies: **FCS_COP.1** Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

5.1.2.3 FCS_CKM.1.C – Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1.C The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *RSA* and specified cryptographic key sizes *RSA –2048 bits* that meet the following: *FIPS PUB 186-2 Digital Signature Standard, Appendix 3.* Alternatively, *ECDSA* key generation is used with *P-256, P-384 and P-521 elliptic curves*

in accordance *FIPS PUB 186-4 Digital Signature Standard, Appendix B.*

Dependencies: FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

Application note: The Encryptor can generate *2048 bit RSA keys* and/or *P-256, P-384 or P-521 elliptic curves*. Correspondingly, CM7 generates *2048 bit RSA keys* and/or *P-256, P-384 or P-521 elliptic curves*.

5.1.2.4 FCS_CKM.2.A – Cryptographic key distribution

Hierarchical to: No other components

FCS_CKM.2.1.A The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method, *RSA public key and KEKs/DEKs using X.509 certificates for authentication* that meets the following: *ATM Forum Security Specification V1.1, PKCS #1*. Alternatively, *ECDSA/ECDH ephemeral key agreement* is used to distribute cryptographic keys in accordance with *NIST SP800-56A*.

Dependencies: FCS_CKM.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

5.1.2.5 FCS_CKM.4 – Cryptographic key destruction

Hierarchical to: No other components

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *All KEKs and DEKs used to encrypt the payload of the Ethernet and Fibre Channel frame are held in volatile memory. Loss of electrical power will destroy all KEKs/DEKs. If the case is opened, then the system master keys (SMK) used to encrypt the RSA/ECDSA private keys and user passwords are automatically erased* that meets the following: *none*.

Dependencies: FCS_CKM.1 Cryptographic key generation

5.1.2.6 FCS_COP.1.A – Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1.A The TSF shall perform *64 bit Cipher Feedback, 8 bit Cipher Feedback, 1 bit Cipher Feedback and counter mode* in accordance with a specified cryptographic algorithm, *DES* and cryptographic key sizes *168 bits* that meet the following: *FIPS PUB 46-3, FIPS PUB 81 and ATM Forum Security Specification V1.1*.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

Application note: Triple DES is used to encrypt the CM7 private key.

5.1.2.7 FCS_COP.1.B – Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1.B The TSF shall perform *self synchronising Cipher Feedback (CFB), counter (CTR) and Galois counter mode (GCM)* in accordance with a specified cryptographic algorithm, *AES*

and cryptographic key sizes *128 bits and 256 bits* that meet the following: *FIPS PUB 197 and NIST SP800-38A*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

5.1.2.8 FCS_COP.1.C – Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1.C The TSF shall perform *public key encryption* in accordance with a specified cryptographic algorithm *RSA* and cryptographic keys of *2048 bits* that meet the following: *ATM Forum Security Specification V1.1, PKCS#1*. Alternatively, *ECDSA/ECDH ephemeral key agreement* using *P-256, P-384 or P-521* elliptic curves is used to establish cryptographic keys in accordance with *NIST SP800-56A*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

Application note: The Encryptor can use 2048 bit RSA keys and P-256, P-384 or P-521 elliptic curves. Correspondingly, CM7 can use 2048 RSA keys and P-256, P-384 or P-521 elliptic curves.

5.1.2.9 FCS_COP.1.F – Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1.F The TSF shall perform *message digest generation/verification* in accordance with a specified cryptographic algorithm *SHA-256* with a cryptographic key size of *256 bits* that meets the following: *FIPS PUB 180-1*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

5.1.2.10 FCS_COP.1.G – Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1.G The TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *RSA* and cryptographic keys of *2048 bits* that meet the following: *PKCS#1*. Alternatively the TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *ECDSA* using *P-256, P-384 or P-521 elliptic curves* in accordance with *FIPS PUB 186-4 Digital Signature Standard*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

Application note: The Encryptor can use *2048 bit RSA keys* and *P-256, P-384 or P-521 elliptic curves*. Correspondingly, CM7 can use *2048 bit RSA keys* and *P-256, P-384 or P-521 elliptic curves*.

5.1.3 User Data Protection (FDP)

5.1.3.1 FDP_ACC.1– Subset access control

Hierarchical to: No other components

FDP_ACC.1.1 The TSF shall enforce the *Management Access Control SFP* on

Subjects: Management packets, consisting of:

- *all SNMPv3 packets received on the encryptor Ethernet management port interface and the local and network interfaces; and*
- *all data received on the encryptor console management port interface*

Objects: Encryptor information, consisting of:

- *Connection Identifier Table;*
- *User Table;*
- *System Time;*
- *Audit Log;*
- *X.509 Certificate(s); and*
- *Firmware.*

Operations: Management operations, consisting of:

- *Viewing Connection Identifier entries, User Table, System Time and Audit Log;*
- *Modifying Connection Identifier entries, User Table and System Time;*
- *Clearing the Audit Log;*
- *X.509 Certificate(s);*
- *Backup and restore encryptor configuration data; and*
- *Upgrading Firmware.*

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.3.2 FDP_ACF.1 – Security attribute based access control

Hierarchical to: No other components

FDP_ACF.1.1 The TSF shall enforce the *Management Access Control SFP* to objects based on the

- *user's ID and the user's authentication password contained in management packets*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If the User ID received on the console port interface is listed in the User Table and the authentication password in the management packet is the same as the local authentication password then console mode logon is allowed. This logon mode will allow management packets to perform the management operations upon the objects allowed by the user's defined role.*
- *If the User ID field in the encrypted SNMPv3 packet is listed in the User Table*

and the authentication password in the management packet is the same as the local authentication password then the management operation is allowed subject to the user's defined role.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- *none.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *following rules*:

- *If the user ID received on the console port interface is not listed in the user table.*
- *If the user ID received on the console port is listed in the user table and the authentication password in the management packet is not the same as the local authentication password.*
- *If the user ID field of the SNMPv3 packet is not listed in the user table.*
- *If the user ID field of the SNMPv3 packet is listed in the user table and the data cannot be decrypted*
- *If the user ID field of the SNMPv3 packet is listed in the user table and the data can be decrypted, but the authentication check fails.*

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.1.3.3 FDP_DAU.1 – Basic data authentication

Hierarchical to: No other components

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *X.509 activation Certificate generation requests from an encryptor and new X.509 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.

Dependencies: No dependencies

5.1.3.4 FDP_IFC.1 – Subset information flow control

Hierarchical to: No other components

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

Subjects: External and internal hosts which send and receive information through the TOE

Information: Ethernet frames and Fibre Channel frames received on the local and network interfaces

Operation: Encrypt, bypass or discard the received Ethernet frames and Fibre Channel frames

Dependencies: FDP_IFF.1 Simple security attributes

5.1.3.5 FDP_IFF.1 – Simple security attributes

Hierarchical to: No other components

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*
- *VLAN ID contained in the Ethernet frame header in VLAN mode*
- *R_CTL and D_ID fields contained in the Fibre Channel frame header*

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:

Subjects on an internal or external network can cause information to flow through the TOE on the local and network interfaces if:

- *The MAC address or VLAN ID in the Ethernet header, R_CTL and D_ID field content contained in the Fibre Channel frame 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 or Fibre Channel frame will be passed with the Ethernet payload, or Fibre channel payload encrypted/decrypted.*
- *If the operation in the CI is defined as “bypass” then the Ethernet frame, or Fibre Channel frame will be passed without modification.*
- *If the operation in the CI is defined as “discard” then the Ethernet frame or Fibre Channel 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.*

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

5.1.3.6 FDP_UCT.1 – Basic data exchange confidentiality

Hierarchical to: No other components

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

Dependencies: FTP_ITC.1 Inter-TSF trusted channel
FDP_IFC.1 Subset information flow control

5.1.4 Identification and Authentication (FIA)

5.1.4.1 FIA_AFL.1 – Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when *three* 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 or surpassed*, the TSF shall *disable the user account for three minutes*.

Dependencies: **FIA_UAU.1** Timing of authentication

5.1.4.2 **FIA_UAU.2 – User authentication before any action**

Hierarchical to: **FIA_UAU.1**

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.

Dependencies: **FIA_UID.1** Timing of identification

5.1.4.3 **FIA_UAU.5 - Multiple authentication mechanisms**

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide *a local password based authentication mechanism and a remote password based authentication mechanism via a TACACS+ server* 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 first and if the user cannot be authenticated the TOE will attempt to authenticate the user via the remote TACACS+ authentication server (if configured)*.

Dependencies: No dependencies

5.1.4.4 **FIA_UID.2 – User identification before any action**

Hierarchical to: **FIA_UID.1**

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.

Dependencies: No dependencies

5.1.5 **Security Management (FMT)**

5.1.5.1 **FMT_MSA.1.A – Management of security attributes**

Hierarchical to: No other components

FMT_MSA.1.1.A The TSF shall enforce the *Information Flow Control SFP* to restrict the ability to *change_default, modify* the security attributes *for each kind of information flow type*:

- *MAC address or VLAN ID for Ethernet information flows*
- *R_CTL and D_ID field contents for Fibre Channel information flows*

And the action applied to the information flow:

- *encrypt, bypass, or discard*

is listed in the CI table to administrators and supervisors.

Dependencies: FDP_IFC.1 Subset information flow control
 FMT_SMR.1 Security roles
 FMT_SMF.1 Specification of Management Functions

5.1.5.2 FMT_MSA.1.B – Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1.B The TSF shall enforce the *Management Access Control SFP* to restrict the ability to:

- *add, delete, or modify* the security attributes *user accounts* to *administrators*
- *activate* the security attributes *X.509 certificates* to *administrators*.
- *remotely upgrade* the security attributes *firmware* to *administrators and upgraders*

Dependencies: FDP_ACC.1 Subset access control
 FMT_SMR.1 Security roles
 FMT_SMF.1 Specification of Management Functions

5.1.5.3 FMT_MSA.3.A – Static attribute initialisation

Hierarchical to: No other components

FMT_MSA.3.1.A 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.A The TSF shall allow the *administrator or supervisor* to specify the alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
 FMT_SMR.1 Security roles

5.1.5.4 FMT_MSA.3.B – Static attribute initialisation

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

FMT_MSA.3.2.B The TSF shall allow the *administrator or supervisor* to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
 FMT_SMR.1 Security roles

5.1.5.5 FMT_MTD.1 – Management of TSF data

Hierarchical to: No other components

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 *administrators*
- *change_default, query, modify, delete and clear* the *CI table and query the User*

Account table to supervisors.

- *query the CI and User Account tables to operators and above*
- *clear the audit log to administrators*
- *set the system time to administrators and supervisors*
- *backup and restore the encryptor configuration data to administrators and supervisors*

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

5.1.5.6 FMT_SMF.1 – Specification of Management Functions

Hierarchical to: No other components

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

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

Dependencies: No dependencies

5.1.5.7 FMT_SMR.1 – Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles *administrator, supervisor, operator and upgrader*.

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

Dependencies: FIA_UID.1 Timing of identification

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_FLS.1 – Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- *self tests return a fail result*

Dependencies: No dependencies

5.1.6.2 FPT_ITT.1 – Basic internal TSF data transfer protection

Hierarchical to: No other components

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

5.1.6.3 FPT_PHP.3.A – Resistance to physical attack

Hierarchical to: No other components

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

Dependencies: No dependencies

5.1.6.4 FPT_PHP.3.B – Resistance to physical attack

Hierarchical to: No other components

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

Dependencies: No dependencies

5.1.6.5 FPT_STM.1 – Reliable time stamps

Hierarchical to: No other components

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

Dependencies: No dependencies

5.1.6.6 FPT_TST.1 – TSF testing

Hierarchical to: No other components.

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.

Dependencies: No dependencies

5.1.7 TOE Access (FTA)

5.1.7.1 FTA_SSL.3 – TSF-initiated termination

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.1.8 Trusted Path/Channels (FTP)

5.1.8.1 FTP_ITC.1 – Inter-TSF trusted channel

Hierarchical to: No other components

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 or 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 and Fibre Channel frames as defined by the Information Flow Control SFP*.

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

The TOE is intended to meet the Common Criteria EAL2+ ALC_FLR.2 evaluation level.

5.3 Security Requirements for the IT Environment

There are no security requirements for the IT environment.

6 TOE Summary Specification

6.1 TOE IT Security Functions

This section presents a high-level summary of the IT security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

IT Security Function	Security Functional Requirements	Description
F.AUDIT	FAU_GEN.1.1 FAU_GEN.1.2 FAU_SAR.1.1 FAU_SAR.1.2 FPT_STM.1.1	<p>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 only, thus there is no requirement for audit logs on CM7. The encryptor is able to generate an audit record for each of the auditable events listed in FAU_GEN.1.1 and FAU_GEN.1.2. The encryptor has a Real Time Clock (RTC) from which a timestamp is obtained to record within each audit record (FPT_STM.1).</p> <p>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 mode presenting the data as a scrolled list of audit text. (FAU_SAR.1)</p> <p>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. Alternatively, the Administrator is permitted to clear the audit log at any time.</p>
F.CERTIFICATE_ MANAGEMENT	FCS_COP.1.1.C FCS_COP.1.1.F FCS_COP.1.1.G FDP_DAU.1.1 FDP_DAU.1.2 FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	<p>The TOE shall manage all necessary tasks to support X.509 certificate based authentication. These tasks are:</p> <ol style="list-style-type: none"> a. Generating and installing signed X.509 certificates into the encryptor b. Authenticating received X.509 certificates using installed trusted CA root certificates <p>Operations relating to generating, X.509 certificates require the use of the RSA or ECDSA algorithms to generate the</p>

IT Security Function	Security Functional Requirements	Description
		<p>private and public key pair (FCS_COP.1.1.C).</p> <p>X.509 certificate signing operations are done using the RSA or ECDSA (FCS_COP.1.1.G) signature algorithms.</p> <p>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 an encryptor which it sends contained within a Senetas proprietary V2 certificate. The encryptor hashes the certificate using SHA-256 (FCS_COP.1.1.F) to create a validation code (FDP_DAU.1.1). 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. (FDP_DAU.1.2). 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.</p> <p>When CM7 returns the encrypted credentials back to the encryptor the same process is repeated again with the CM7 user and remote operator agreeing that the validation codes are the same before the default user account is updated by the encryptor.</p> <p>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.</p> <p>Now 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 certificate(s) to establish trusted communications channels between itself and other Encryptors (remote trusted IT products). Both encryptors must have a valid X.509 certificate(s), in which the root trust anchor can be validated</p>

IT Security Function	Security Functional Requirements	Description
		(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.1.1.F),
F.DATA_EXCHANGE	FCS_COP.1.1.B FDP_UCT.1.1	<p>The TOE encrypts the payload on the basis of the address in the ethernet frame or the contents of the R_CTL and D_ID fields in the fibre channel frame and whether the CI entry requires encryption of traffic on that address or frame type.</p> <p>If encryption is required, the encryptor performs hardware- or software based 128 or 256 bit AES encryption in CFB, counter mode, or GCM on the Ethernet frame payload or hardware based 256 bit AES encryption in CFB mode on the fibre channel payload and a user configurable portion of the header (FDP_UCT.1).</p> <p>The various models use the following encryption methods and algorithms (FCS_COP.1.B):</p> <ul style="list-style-type: none"> • 10/100/1000 Ethernet uses AES with 128 or 256 bit key using the self synchronising CFB, counter mode or GCM (CN8000/ CN6040/ CN6010/ CN4020/ CN4010) • 10 Gigabit Ethernet uses AES with 128 or 256 bit key using counter mode or GCM (CN8000/CN6100) • Fibre Channel uses AES with 256 bit key using the self-synchronising CFB mode (CN8000/CN6040)
F.IDENTIFICATION	FIA_AFL.1.1 FIA_AFL.1.2 FIA_UAU.2.1 FIA_UAU.5.1 FIA_UID.2.1	<p>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. Identification & Authentication services are only performed by the encryptor.</p> <p>All user passwords must have a minimum length of eight characters. The set of possible characters are A-Z, a-z, 0-9 and ` ~ ! @ # \$ % ^ & * () _ - + = { [] } ; : ' " , < . > ? / \.</p>

IT Security Function	Security Functional Requirements	Description
		<p>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, and the event is audited. After three consecutive unsuccessful logon attempts the user account will be disabled for three minutes (FIA_AFL.1). 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 RSA and ECDSA. RSA Keys must be a minimum of 2048 bits and ECDSA is restricted to NIST P-256, P-384 and P-521 curves.</p> <p>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 (and optionally encrypted) 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. 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, and the event is audited. Each SNMPv3 packet received is</p>

IT Security Function	Security Functional Requirements	Description
		<p>identified and authenticated in this way.</p> <p>When configured user authentication can be performed via a centralised TACACS+ server. When a user attempts to log onto an encryptor via either the CLI or CM7 the encryptor will first compare the supplied user credentials against the locally stored credentials in the user table. If a match is found the user will be granted access to the encryptor. If a match is not found and a remote TACACS+ server is configured the user's credentials will be verified against the database on the remote server. If an exact match of the user credentials are found on the remote server the user will be granted access to the encryptor.</p>

IT Security Function	Security Functional Requirements	Description
<p>F.KEY_ MANAGEMENT</p>	<p>FCS_CKM.1.1.A FCS_CKM.1.1.B FCS_CKM.1.1.C FCS_CKM.2.1.A FCS_CKM.4.1 FCS_COP.1.1.A</p>	<p>The TOE shall manage all the necessary keys and mechanisms to support its cryptographic operations, namely:</p> <ul style="list-style-type: none"> a. Generating public/private key pairs for both CM7 and encryptors. (FCS_CKM.1.1.C) b. Generating and securely transferring KEKs between encryptors. (FCS_CKM.1.1.A) Keys are distributed between encryptors using RSA public key cryptography and X.509 certificates are used for authentication. Alternatively, ECDSA/ECDH ephemeral key agreement is used to distribute cryptographic keys in accordance with NIST SP800-56A (FCS_CKM.2.1.A). c. Updating DEKs used for AES encryption between encryptors. (FCS_CKM.2.1.A) AES DEKs are periodically updated according to local security policy requirements set by Administrators or Supervisors. d. Generating a shared secret via a Diffie-Hellman Key-Agreement for SNMPv3 management. (FCS_CKM.1.1.B) e. Protecting user passwords used for protecting authentication keys, during user account setup on an encryptor, by encrypting the password data with the System Master Key of the intended encryptor that will operate the user account. The encryption is performed using 3DES (FCS_COP.1.1.A) with the generated 3DES keys (FCS_CKM.1.1.A). f. KEKs and DEKs held in volatile memory (RAM) are erased on loss of power (FCS_CKM.4).

IT Security Function	Security Functional Requirements	Description
F.INFORMATION_ FLOW_ CONTROL	FDP_IFC.1.1 FDP_IFF.1.1 FDP_IFF.1.2 FDP_IFF.1.3 FDP_IFF.1.4 FDP_IFF.1.5 FDP_IFF.1.6 FMT_MSA.3.1.A FMT_MSA.3.2.A	<p>The TOE shall control the flow of Ethernet frames or Fibre Channel frames received on the private network interface and on the public network interface from external hosts on the basis of the address or VLAN ID in the Ethernet frame or the contents of the R_CTL and D_ID fields in the Fibre Channel frame (FDP_IFC.1, FDP_IFF.1.1).</p> <p>In doing so, the TOE shall take one of four possible actions, encrypt the payload, decrypt the payload, pass the payload unchanged, or discard the payload (FDP_IFC.1, FDP_IFF.1.1).</p> <p>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 by default (FDP_IFC.1, FDP_IFF.1.1).</p> <p>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 (FMT_MSA.3.A).</p>
F.ROLE_ BASED_ ACCESS	FDP_ACC.1.1 FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4 FMT_MSA.1.1.B FMT_MSA.3.1.B FMT_MSA.3.2.B FMT_MTD.1.1 FMT_SMR.1.1 FMT_SMR.1.2 FTA_SSL.3.1 FMT_MSA.1.1.A FMT_SMF.1.1	<p>The TOE can be accessed and managed using SNMPv3 packets received on the Ethernet management port interface and network interface or via the console management port interface. The encryptor's USB port can be used to upgrade firmware (FDP_ACC.1).</p> <p>Users will be allowed access to the TOE when a valid user ID and password are provided (FDP_ACF.1.1). 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 (FDP_ACF.1.2, FDP_ACF.1.3). If any of these conditions are not met then access will be denied (FDP_ACF.1.4). The TOE defines three roles for accessing the TSFs (FDP_ACC.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). These are:</p> <p>Administrators: Who can change defaults, query,</p>

IT Security Function	Security Functional Requirements	Description
		<p>modify, delete and clear the CI entries (FMT_MSA.1.1.A), User accounts, activate X.509 certificates, clear the audit log, view the audit log, set the system time and backup and restore the encryptor configuration data and remotely upgrade the firmware (FMT_MSA.1.B) via either SFTP or FTPS.</p> <p>Supervisors: Who can change defaults, query, modify, delete and clear the CI entries (FMT_MSA.1.1.A), view the User accounts table and audit log and set the system time (FMT_MSA.1.B).</p> <p>Operators: Who can query the CI and User Account tables only, and view the audit log.</p> <p>Upgraders: Who can remotely upgrade the firmware via either USB, SFTP or FTPS, query the CI and User Account tables and view the audit log.</p> <p>When the TOE is accessed the TOE associates users with these roles and prevents a user from performing operations on the TSF's that they are not authorised to perform (FMT_SMR.1).</p> <p>The console user session will be automatically terminated by the encryptor after a period of 10 minutes as a result of user inactivity (FTA_SSL.3).</p> <p>The User Table initially has one default administrator account. By default all other users are created as operators unless the administrator overrides this value (FMT_MSA.3.B)</p>

IT Security Function	Security Functional Requirements	Description
F.SECURE_REMOTE_MANAGEMENT	FPT_ITT.1.1 FCS_COP.1.1.B	<p>The TOE shall protect the confidentiality of remote management data between the encryptors and the CM7 remote management station. (FPT_ITT.1)</p> <p>The TOE can encrypt SNMPv3 data packets using 128-bit AES with keys derived from the Engine ID of the encryptor being managed and the user's privacy key. (FCS_COP.1.B)</p> <p>The user initiates the remote management session by executing the CM7 software on their workstation.</p>
F.SELF_PROTECT	FCS_CKM.4.1 FPT_FLS.1.1 FPT_PHP.3.1.A FPT_PHP.3.1.B FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3 FCS_COP.1.1.A	<p>The TOE protects itself from attempts to get access to the user passwords (FPT_PHP.3.B) and key material (FPT_PHP.3.A) stored within the encryptor. An erase mechanism is provided that is activated whenever the case is opened. Once activated, the System Master key (SMK) is erased from battery-backed volatile memory (FCS_CKM.4).</p> <p>The System Master Key (SMK) encrypts all private key material and user password data, and so removal of the System Master Key (SMK) means the encrypted data cannot be accessed.</p> <p>The encryptor performs self-tests during start-up to check that the underlying functionality of the TSF is functioning correctly (FPT_TST.1). The tests include verification of the cryptographic processors, Random Noise Source, Firmware integrity, System Memory, Software integrity, as well as TSF configuration data. 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 (FPT_FLS.1).</p> <p>The TOE protects its own private key on CM7 by encrypting the private key using triple DES and a passphrase (FCS_COP.1.A). Only a user who has access to the passphrase can unlock the private key of the CM7.</p>

Table 8 – TOE IT Security Functions

7 Rationale

7.1 Security Objectives Rationale

7.1.1 Mapping of Threats, OSPs and Assumptions to Security Objectives

The following table demonstrates that the each threat, OSP and assumption is addressed by at least one security objective, and each security objective addresses at least one threat, OSP or assumption.

Objectives	O.ADMIN	O.AUDIT	O.AUDITLOG	O.AUTHDATA	O.CERTGEN	O.CONNECT	O.ENCRYPT	O.FAILSAFE	O.INFOFLOW	O.IDENT	O.INSTALL	O.KEYMAN	O.PERSONNEL	O.PHYSICAL	O.REMOTEMGT	O.ROLES	O.TAMPER	O.ROLEMGT
ASSUMPTIONS																		
A.ADMIN													✓					
A.AUDIT			✓															
A.CM											✓			✓				
A.INSTALL											✓							
A.LOCATE											✓			✓				
A.PRIVATEKEY				✓														
THREATS																		
T.ABUSE		✓	✓	✓						✓			✓			✓		✓
T.ATTACK	✓	✓	✓					✓								✓		✓
T.CAPTURE							✓		✓			✓						
T.CONNECT					✓	✓			✓			✓						
T.IMPERSON	✓	✓	✓	✓						✓								
T.LINK					✓		✓		✓			✓						
T.MAL								✓										
T.OBSERVE												✓			✓			
T.PHYSICAL											✓		✓	✓			✓	
T.PRIVILEGE		✓	✓	✓						✓			✓			✓		✓
OSP'S																		
P.CRYPTO					✓		✓					✓			✓			
P.INFOFLOW	✓								✓									
P.ROLES	✓															✓		✓

Table 9 – Mapping of Threats, OSPs and Assumptions to Security Objectives

7.1.2 Informal argument of adequacy and correctness of mapping

7.1.2.1 Assumptions

Assumption	Description
A.ADMIN	<i>O.PERSONNEL</i> ensures that only trusted and competent administrators are authorised to manage the TOE.
A.AUDIT	<i>O.AUDITLOG</i> ensures that the facilities to effectively manage audit information are provided.
A.CM	<p><i>O.INSTALL</i> ensures that the CM7 Management Station is installed and managed in a secure environment.</p> <p><i>O.PHYSICAL</i> ensures that the CM7 Management Station will be protected from physical attacks</p> <p>The combination of these objectives will prevent unauthorised users from attempting to compromise the security functions of the CM7 Management Station and therefore cover this assumption.</p>
A.INSTALL	<i>O.INSTALL</i> ensures that the TOE is delivered, installed, managed and operated in a manner that maintains security.
A.LOCATE	<i>O.INSTALL</i> ensures that encryptors are installed correctly in a secure environment while <i>O.PHYSICAL</i> ensures that this environment remains secure from unauthorised people.
A.PRIVATEKEY	<i>O.AUTHDATA</i> ensures that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account. The authentication data includes the passphrase to protect the CM7's private key.

Table 10 – Informal argument of assumptions

7.1.2.2 Threats

Threat	Justification
<p>T.ABUSE</p>	<p><i>O.AUDIT</i> provides a means of recording security relevant events and <i>O.AUDITLOG</i> ensures that the facilities to effectively manage audit information are provided. This allows authorised users to detect modifications. This will prevent compromises being undetected.</p> <p><i>O.ROLES</i> ensures the user can only access the operations that the role authorises. <i>O.ROLEMGT</i> ensures that users are allocated roles with <i>least privilege</i>. This can minimise the threat damage caused by the role.</p> <p><i>O.IDENT</i> ensures that all users are uniquely identified and authenticated before access to TOE management features is allowed. <i>O.AUTHDATA</i> ensures that the authentication data for each account on the TOE is held securely and not disclosed to persons unauthorised to use that account. So 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 (<i>O.AUDIT</i> and <i>O.AUDITLOG</i>) will deter users from intentionally abusing their privileges.</p> <p><i>O.PERSONNEL</i> supports the above objectives by ensuring 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 compromising information.</p> <p>The combination of these objectives will reduce this threat to an acceptable level.</p>

Threat	Justification
T.ATTACK	<p><i>O.AUDIT</i> provides a means of recording security relevant events and <i>O.AUDITLOG</i> ensures that the facilities to effectively manage audit information are provided. This allows authorised users to detect modifications. This will prevent compromises being undetected.</p> <p><i>O.ROLES</i> ensures the user can only access the operations that the role authorises. <i>O.ROLEMGT</i> ensures that users are allocated roles with <i>least privilege</i>. This prevents insider users from doing operations for which they are not authorised.</p> <p><i>O.ADMIN</i> ensures that only authorised users can access the TOE management functions. This prevents outsider attackers from accessing the TOE management functions and compromising information.</p> <p><i>O.FAILSAFE</i> ensures that if an error occurs the TOE will preserve a secure state. If a logical attack results in an error condition, then the TOE will not compromise information.</p> <p>The combination of these objectives is sufficient to reduce undetected logical attacks from insiders and outsiders to an acceptable level.</p>
T.CAPTURE	<p><i>O.INFOFLOW</i> allows for selected Ethernet frames or Fibre Channel frames to be encrypted or discarded according to a defined security policy and therefore preventing capture on the public network.</p> <p><i>O.ENCRYPT</i> allows for the encryption of Ethernet payloads or Fibre Channel payloads and a user configurable portion of the Fibre Channel Frame header ensuring that captured data can not be readable without private keys.</p> <p><i>O.KEYMAN</i> ensures the DEKs used to encrypt the payloads for <i>O.ENCRYPT</i> are kept private by using secure key generation, distribution, agreement, encryption, destruction and exchange techniques.</p> <p>When these objectives are met, the threat of confidential information being recovered by an attacker will suitably diminish.</p>

Threat	Justification
<p>T.CONNECT</p>	<p><i>O.INFOFLOW</i> allows authorised users to explicitly allow connections, however, by default all connections, other than Ethernet management frames, Fibre Channel management frames and selected Fibre Channel link management frames to the TOE, will be discarded.</p> <p><i>O.KEYMAN</i> ensures that encrypted connections cannot be made unless the originator and receiver hold a valid X.509 certificate signed by a trusted CA. This will prevent connections with untrusted networks from being established.</p> <p><i>O.CERTGEN</i> supports <i>O.KEYMAN</i> by ensuring the TOE has the capability to generate, issue and manage X.509 certificates.</p> <p><i>O.CONNECT</i> supports the environment to ensure that connections that would undermine security are not established by those responsible for the TOE.</p> <p>When all these objectives are met, the threat of an insecure connection being created by an attacker will be suitably diminished.</p>
<p>T.IMPERSON</p>	<p><i>O.IDENT</i> uniquely identifies all users and authenticates the claimed identity before granting a user access to the TOE management facilities. For an attacker to impersonate an authorised user, the attacker must know the user's identity and authentication data. To restrict opportunities for impersonation attacks accounts are disabled on authentication failure</p> <p><i>O.AUTHDATA</i> ensures that users are responsible not to disclose their authentication data so attackers cannot impersonate authorised users.</p> <p><i>O.ADMIN</i> ensures only authorised users can manage the TOE and its security features.</p> <p><i>O.AUDIT</i> provides a means of recording security relevant events and <i>O.AUDITLOG</i> ensures that the facilities to effectively manage audit information are provided. This allows authorised users to detect when impersonation attacks (eg. brute force password guessing) occur.</p> <p>When all these objectives are met, the threat of privileged users being impersonated by an inside or outside attacker will suitably diminish.</p>

Threat	Justification
T.LINK	<p><i>O.INFOFLOW</i> allows authorised users to explicitly allow connections, however, by default, all connections to the TOE will be discarded.</p> <p><i>O.ENCRYPT</i> allows for the encryption of Ethernet and Fibre Channel payloads.</p> <p><i>O.KEYMAN</i> 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 <i>O.CERTGEN</i>. So <i>O.KEYMAN</i> and <i>O.CERTGEN</i> restrict the number of possible communications paths to only other authorised encryptors.</p> <p>The objectives <i>O.INFOFLOW</i>, <i>O.KEYMAN</i> and <i>O.CERTGEN</i> 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 <i>O.ENCRYPT</i>, 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.</p>
T.MAL	<p><i>O.FAILSAFE</i> ensures that the TOE will enter a secure state if any malfunction of the TOE is detected.</p>
T.OBSERVE	<p><i>O.REMOTEMGT</i> ensures that remote management sessions can be encrypted. This will minimise the threat that an attacker may observe legitimate management communications, as the data would have to be decrypted with secret DEKs.</p> <p><i>O.KEYMAN</i> supports <i>O.REMOTEMGT</i> to allow cryptographic key management to enable cryptographic exchanges between the encryptor and CM7.</p> <p>When all these objectives are met, the threat of legitimate management communications being observed by an attacker will be suitably diminished.</p>

Threat	Justification
<p>T.PHYSICAL</p>	<p><i>O.INSTALL</i> ensures that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.</p> <p><i>O.PHYSICAL</i> ensures that those parts of the TOE that are critical to security policy enforcement are protected from physical attack.</p> <p><i>O.PERSONNEL</i> ensures that those responsible for the TOE are competent to manage the TOE and can be trusted not to deliberately abuse their privileges.</p> <p>The above environmental objectives provide a secure environment for the TOE to reduce a physical attack from occurring.</p> <p><i>O.TAMPER</i> provides physical protection of stored assets (user authentication and cryptography key material) to prevent a security compromise via physical means if the above environmental measures are not sufficient.</p> <p>With all objectives met, this threat is removed.</p>
<p>T.PRIVILEGE</p>	<p><i>O.ROLES</i> ensures the user can only access the operations that the role authorises. <i>O.ROLEMGT</i> ensures that users are allocated roles with <i>least privilege</i>. This limits the operations and therefore the damage a compromise can lead to.</p> <p><i>O.PERSONNEL</i> ensures that users within the environment are trusted and competent. This will minimise the threats from hostile or wilfully negligent administrators.</p> <p><i>O.IDENT</i> ensures that a user requesting information is correctly identified. While <i>O.AUTHDATA</i> ensures that they are responsible with that information by not disclosing it to users so those people authorised to use the account can be held responsible for their actions.</p> <p><i>O.AUDIT</i> provides a means of recording security relevant events and <i>O.AUDITLOG</i> ensures that the facilities to effectively manage audit information are provided. This allows authorised users to monitor possible changes to the configuration of the TOE, allowing all authorised users to detect modifications. The user's identity from <i>O.IDENT</i> will be recorded in the audit log, so privileged users will have their actions recorded and reviewed to deter them from abusing their privileges.</p> <p>When all these objectives are met, the threat of privileged users compromising information is suitably diminished.</p>

Table 11 – Informal argument of threats

7.1.2.3 Policies

Policy	Description
P.CRYPTO	<i>O.ENCRYPT</i> , <i>O.KEYMAN</i> , <i>O.REMOTEMGT</i> and <i>O.CERTGEN</i> provide the confidentiality, authentication and key management services specified by this organisational security policy.
P.INFOFLOW	<i>O.INFOFLOW</i> provides the traffic flow control specified in the organisational security policy. <i>O.ADMIN</i> ensures that only authorised users can set the traffic control as specified in the organisational security policy.
P.ROLES	<i>O.ROLEMGT</i> ensures that administrators will allocate users to distinct roles on the basis of least privilege. <i>O.ROLES</i> ensures that users can only perform the operations for which their role is explicitly authorised. <i>O.ADMIN</i> ensures that only authorised users can manage the TOE as specified in the organisational security policy.

Table 12 – Informal argument of policies

7.1.2.4 Rationale

Given the arguments in the above tables and the mappings shown in Table 9, it has been demonstrated that the security objectives are suitable to counter all threats and to consider all assumptions and organisational security policies.

7.2 Security Requirements Rationale

7.2.1 Mapping of Security Functional Requirements to Security Objectives

The following table demonstrates that each TOE SFR is mapped to at least one TOE security objective.

Security Objective Security Functional Requirement	O.ADMIN	O.AUDIT	O.CERTGEN	O.ENCRYPT	O.FAILSAFE	O.INFOFLOW	O.IDENT	O.KEYMAN	O.REMOTEMGT	O.ROLES	O.TAMPER
FAU_GEN.1.1		✓									
FAU_GEN.1.2		✓									
FAU_SAR.1.1		✓									
FAU_SAR.1.2		✓									
FCS_CKM.1.1.A								✓			
FCS_CKM.1.1.B								✓			
FCS_CKM.1.1.C								✓			
FCS_CKM.2.1.A								✓			
FCS_CKM.4.1								✓			✓
FCS_COP.1.1.A											✓
FCS_COP.1.1.B				✓					✓		
FCS_COP.1.1.C			✓					✓			
FCS_COP.1.1.F			✓								
FCS_COP.1.1.G			✓								
FDP_ACC.1.1	✓										
FDP_ACF.1.1	✓										
FDP_ACF.1.2	✓										
FDP_ACF.1.3	✓										
FDP_ACF.1.4	✓										
FDP_DAU.1.1			✓								
FDP_DAU.1.2			✓								
FDP_IFC.1.1						✓					
FDP_IFF.1.1						✓					
FDP_IFF.1.2						✓					
FDP_IFF.1.3						✓					
FDP_IFF.1.4						✓					
FDP_IFF.1.5						✓					
FDP_UCT.1.1				✓							
FIA_AFL.1.1							✓				

Security Objective Security Functional Requirement	O.ADMIN	O.AUDIT	O.CERTGEN	O.ENCRYPT	O.FAILSAFE	O.INFOFLOW	O.IDENT	O.KEYMAN	O.REMOTEMGT	O.ROLES	O.TAMPER
FIA_AFL.1.2							✓				
FIA_UAU.2.1							✓				
FIA_UID.2.1							✓				
FMT_MSA.1.1.A						✓					
FMT_MSA.1.1.B										✓	
FMT_MSA.3.1.A						✓					
FMT_MSA.3.1.B										✓	
FMT_MSA.3.2.A						✓					
FMT_MSA.3.2.B										✓	
FMT_MTD.1.1	✓									✓	
FMT_SMR.1.1										✓	
FMT_SMR.1.2										✓	
FMT_SMF.1.1	✓										
FPT_FLS.1.1					✓						
FPT_ITT.1.1									✓		
FPT_PHP.3.1.A											✓
FPT_PHP.3.1.B											✓
FPT_STM.1.1		✓									
FPT_TST.1.1					✓						
FPT_TST.1.2					✓						
FPT_TST.1.3					✓						
FTA_SSL.3.1	✓										
FTP_ITC.1.1			✓								
FTP_ITC.1.2			✓								
FTP_ITC.1.2			✓								

Table 13 – Mapping of Security Functional Requirements to Security Objectives

7.2.2 Informal Argument of Sufficiency

The following table contains a justification for the chosen SFRs and their suitability to satisfy each security objective for the TOE.

Objective	Security Functional Requirement	Justification
O.ADMIN	FDP_ACC.1.1 FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4 FTA_SSL.3.1 FMT_MTD.1.1 FMT_SMF.1.1	<p><i>FDP_ACC.1.1</i>, <i>FDP_ACF.1.1</i>, <i>FDP_ACF.1.2</i>, <i>FDP_ACF.1.3</i> and <i>FDP_ACF.1.4</i> together provide the capability for management of the TOE security functions by authorised users in a manner required for correct operation and management of the TOE as required by <i>O.ADMIN</i>.</p> <p><i>FTA_SSL.3.1</i> provide additional protection automatically terminating management sessions after a period of user inactivity.</p> <p><i>FMT_MTD.1.1</i> provides the function so authorised roles can manage the TSF data.</p> <p><i>FMT_SMF.1.1</i> provides security management of attributes and data to allow administration of the TOE.</p>
O.AUDIT	FAU_GEN.1.1 FAU_GEN.1.2 FAU_SAR.1.1 FAU_SAR.1.2 FPT_STM.1.1	<p><i>FAU_GEN.1.1</i> and <i>FAU_GEN.1.2</i> provide the capability for generating and recording audit events in the manner required by <i>O.AUDIT</i>.</p> <p><i>FAU_SAR.1.1</i> and <i>FAU_SAR.1.2</i> provide the capability for viewing audit logs to support the effective use and management of the audit facilities in a manner required by <i>O.AUDIT</i>.</p> <p><i>FPT_STM.1.1</i> ensures that a date and time stamp is recorded with the audit record. If the user sets a timezone other than UTC then to guarantee the accuracy of time stamps the following procedure should be applied. With the timezone set to UTC set the time to UTC time and then change the timezone to the required location.</p>

Objective	Security Functional Requirement	Justification
O.CERTGEN	FCS_COP.1.1.C FCS_COP.1.1.F FCS_COP.1.1.G FDP_DAU.1.1 FDP_DAU.1.2 FTP_ITC.1.1 FTP_ITC.1.2 FTP_ITC.1.3	<p><i>FCS_COP.1.1.C</i> uses the RSA algorithm to encrypt the RSA private key for X.509 certificates.</p> <p><i>FCS_COP.1.1.G</i> together with <i>FCS_COP.1.1.F</i> provides the means for signing completed X.509 certificates for the encryptor. These cryptographic functions meet the standards required by FIPS 140-2 and ISM.</p> <p><i>FDP_DAU.1.1</i> and <i>FDP_DAU.1.2</i> provides the means for producing a digest of the data for authentication purposes, when generating partial X.509 certificates in activation mode, and after sending completed and signed X.509 certificates from CM7 to the encryptor. Activation provides for secure replacement of the default user credentials.</p> <p><i>FTP_ITC.1.1</i>, <i>FTP_ITC.1.2</i> and <i>FTP_ITC.1.3</i> provides the means for using the X.509 certificates to authenticate other encryptors and establish a secure trusted channel.</p>
O.ENCRYPT	FCS_COP.1.1.B FDP_UCT.1.1	<p><i>FCS_COP.1.1.B</i> and <i>FDP_UCT.1.1</i>, together provide the capability for encrypting information to protect the confidentiality of information transferred across the Ethernet or Fibre Channel data networks, as required by O.ENCRYPT.</p> <p>The cryptographic functions meet the standards required by FIPS 140-2 and ISM.</p>
O.FAILSAFE	FPT_FLS.1.1 FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3	<p><i>FPT_FLS.1.1</i> together with <i>FPT_TST.1.1</i>, <i>FPT_TST.1.2</i> and <i>FPT_TST.1.3</i> provides 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.</p>

Objective	Security Functional Requirement	Justification
O.INFOFLOW	FDP_IFC.1.1 FDP_IFF.1.1 FDP_IFF.1.2 FDP_IFF.1.3 FDP_IFF.1.4 FDP_IFF.1.5 FMT_MSA.1.1.A FMT_MSA.3.1.A FMT_MSA.3.2.A	<p><i>FDP_IFC.1.1</i>, <i>FDP_IFF.1.1</i>, <i>FDP_IFF.1.2</i>, <i>FDP_IFF.1.3</i>, <i>FDP_IFF.1.4</i>, <i>FDP_IFF.1.5</i>, <i>FMT_MSA.1.1.A</i>, <i>FMT_MSA.3.1.A</i> and <i>FMT_MSA.3.2.A</i> together provide the capability for authorised users to control traffic flow between subjects using the Ethernet MAC address or VLAN ID or the contents of the R_CTL and D_ID fields in the Fibre Channel frame in a manner required by O.INFOFLOW.</p>
O.IDENT	FIA_UAU.2.1 FIA_UID.2.1 FIA_AFL.1.1 FIA_AFL.1.2	<p><i>FIA_UAU.2.1</i> and <i>FIA_UID.2.1</i> provide the capability for identifying and authenticating all users in a manner required by O.IDENT.</p> <p><i>FIA_AFL.1.1</i> and <i>FIA_AFL.1.2</i> provide additional protection by limiting the number of unsuccessful authentication attempts before imposing a timeout on that user account.</p>
O.KEYMAN	FCS_COP.1.1.C FCS_CKM.1.1.A FCS_CKM.1.1.B FCS_CKM.1.1.C FCS_CKM.2.1.A FCS_CKM.4.1	<p><i>FCS_CKM.1.1.A</i>, <i>FCS_CKM.1.1.B</i>, <i>FCS_CKM.1.1.C</i>, <i>FCS_CKM.2.1.A</i>, and <i>FCS_CKM.4.1</i> 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.KEYMAN.</p> <p><i>FCS_COP.1.1.C</i> provides RSA encryption of KEKs or ECDH generation of DEKs.</p> <p>These cryptographic functions meet the standards required by FIPS 140-2 and ISM.</p>
O.REMOTEMGT	FCS_COP.1.1.B FPT_ITT.1.1	<p><i>FCS_COP.1.1.B</i>, provides the capability for encryption methods for management data over the network.</p> <p><i>FPT_ITT.1.1</i> ensures the confidentiality of remote management information is maintained.</p>

Objective	Security Functional Requirement	Justification
O.ROLES	FMT_MSA.1.1.B FMT_MSA.3.1.B FMT_MSA.3.2.B FMT_MTD.1.1 FMT_SMR.1.1 FMT_SMR.1.2	<p><i>FMT_SMR.1.1</i> specifies the three possible roles administrator, supervisor and operator.</p> <p><i>FMT_MSA.1.1.B, FMT_MSA.3.1.B, FMT_MSA.3.2.B</i> defines each role's privileges for managing the TSF security attributes.</p> <p><i>FMT_MTD.1.1</i> defines each role's privileges for managing the TSF data.</p> <p><i>FMT_SMR.1.2</i> associates a human with one role.</p> <p>In combination, these SFRs restricts the human's access to only those TSF attributes, data and operations explicitly allowed by the associated role.</p>
O.TAMPER	FPT_PHP.3.1.A FPT_PHP.3.1.B FCS_COP.1.1.A FCS_CKM.4.1	<p><i>FPT_PHP.3.1.A and FPT_PHP.3.1.B</i> provides the capability for the TOE to physically protect itself from compromise of key material and user authentication data via physical access to the TOE as required by O.TAMPER.</p> <p><i>FCS_COP.1.1.A</i> provides the capability for the TOE to encrypt the private keys and user passwords using 3DES.</p> <p><i>FCS_CKM.4.1</i> provides the capability to delete the System Master key (SMK) by disconnection of battery as key is held in battery-backed volatile memory.</p>

Table 14 – Informal Argument of Sufficiency

Given the arguments in Table 14 and the mappings shown in Table 13, it has been demonstrated that the security functional requirements are sufficient to enforce the security objectives for the TOE.

7.2.3 Rationale for EAL2+ ALC_FLR.2 Assurance level

In Part 3 of the CC EAL2 is defined as “methodically designed, tested and reviewed”. This assurance level is therefore applicable in those circumstances where users require a methodically designed, tested, and reviewed product and also require a moderate to high level of independently assured security in conventional commodity security products and are prepared to incur additional security-specific engineering costs.

EAL2 assurance level has been chosen for the TOE as it is considered appropriate for the protection of sensitive information transmitted over public Ethernet and point-to-point Fibre channel data networks. It is also

considered to be an appropriate level to counter the threats outlined in section 3 and to satisfy the security objectives listed in section 4.

Senetas has chosen to augment EAL 2 by adding the assurance component ALC_FLR.2 to assure that TOE users will know how to report security flaws, and that Senetas will act appropriately to address security flaws.