Security Target for
CypherNET Ethernet Encryptor
CypherNET Fibre Channel Encryptor
CypherStream Ethernet Encryptor
CypherManager

Compliant to the Common Criteria

Version

Version 2.00	4-Aug-09	Update CypherStream firmware version to 1.0.6 Finalise ST for release

Table of Contents

List of Tables

List of Figures

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:

- CypherNET encryptors;
- CypherStream encryptors; and
- CypherManager.

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

CypherNET is a high-speed, standards based multi-protocol encryptor 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.

CypherStream is a small desktop form factor 10 Mbps Ethernet Encryptor designed to provide an integrated data security solution for point to point or meshed Ethernet links up to 10 Mbps. CypherStream has been designed to integrate transparently and simply into network architectures.

CypherManager is a Graphical User Interface (GUI) software package that runs on Windows platforms. It acts as a Certification Authority (CA) for signing X.509 certificates and provides secure remote installation of X.509 certificates into CypherNET and CypherStream using SNMPv3.

CypherManager can also be used to securely remotely manage CypherNet and CypherStream encryptors. It can be used to securely set and monitor CypherNet and CypherStream internal configuration parameters.

IdQuantique have developed a quantum key distribution system (QKD) to generate and exchange cryptographic keys over fiber optic networks with absolute security. The QKD keys can be provided to CypherNet encryptors as input into session keys for data encryption. This combination of IdQuantique and CypherNet is known as Cerberis. Although the IdQuantique product is not in the scope of the TOE, the CypherNet encryptor using QKD keys is in scope.

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 EAL4+ 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.

1.4.2 Security Target Identification

ST Title: CypherNET Security Target

ST Version: 2.00

ST Issue Date: Aug-09

1.4.3 TOE Identification

CypherNET Ethernet, CypherNet Fibre Channel, and CypherStream models are marketing names used to describe specific derivations of CypherNET, which have restricted functionality. Any reference to CypherNET in this document also applies to these models.

CypherNet Model numbers applicable to this evaluation are listed in Table 2 and **Error! Reference source not found.**.

CypherStream Model numbers applicable to this evaluation are listed in Table 3.

The CypherNet and CypherStream Application Software and CypherManager versions pertinent to this evaluation are as follows:

Description	Version	Applicable CypherNet and CypherStream Model Numbers
CypherNet Application Software	2.0.0	Applies to all units
CypherStream Application Software	1.0.6	Applies to all units
CypherManager	6.5.0	Applies to all units

Table 1 – CypherNet and CypherStream Application Software and CypherManager Versions

1.4.4 CypherNET Models

ID	Description
A5137B	CYPHERNET ETHERNET 100M (SFP+RJ45) AC UNIT
A5139B	CYPHERNET ETHERNET 10M (SFP+RJ45) AC UNIT
A5141B	CYPHERNET ETHERNET 1G (SFP+RJ45) AC UNIT
A5171B	CYPHERNET FIBRE CHANNEL 1G AC UNIT
A5173B	CYPHERNET FIBRE CHANNEL 2G AC UNIT
A5175B	CYPHERNET FIBRE CHANNEL 4G AC UNIT
A5203B	CYPHERNET ETHERNET 10G AC UNIT
A5204B	CYPHERNET ETHERNET 10G DC UNIT
A2153B	CYPHERNET ETHERNET 10M AC UNIT
A2151B	CYPHERNET ETHERNET 100M AC UNIT
A2101B	CYPHERNET ETHERNET 1G AC UNIT
A2159B	CYPHERNET ETHERNET 10M (SFP+RJ45) AC UNIT
A2157B	CYPHERNET ETHERNET 100M (SFP+RJ45) AC UNIT
A2155B	CYPHERNET ETHERNET 1G (SFP+RJ45) AC UNIT
A2165B	CYPHERNET FIBRE CHANNEL 1G AC UNIT
A2163B	CYPHERNET FIBRE CHANNEL 2G AC UNIT
A2161B	CYPHERNET FIBRE CHANNEL 4G AC UNIT
A2202B	CYPHERNET ETHERNET 10G DC UNIT

Table 2 – CypherNET Model Numbers

1.4.5 CypherStream Models

ID	Description
A4201B	CYPHERSTREAM ETHERNET 10M (RJ45) AC UNIT

Table 3 – CypherStream Model Numbers

1.4.6 QKD models

A valid Cerberis configuration requires the following IdQuantique device:

ID	Description
5100	CERBERIS QUANTUM KEY DISTRIBUTION SYSTEM

Table 4 – Cerberis Model Numbers

1.5 References

1. Common Criteria for Information Technology Security Evaluation. Version 3.1, September 2007
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

1.6 Glossary of Key Terms

CA	Certification Authority
CC	Common Criteria
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
MASTER KEY	Key used to encrypt session keys
Mbps	Megabits per second
OSP	Organisational Security Policy
PP	Protection Profile
RFC	Request for Comment
RSA	Public Key Algorithm
SESSION KEY	Key used to encrypt defined segments of user data traffic
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SNMPv3	Simple Network Management Protocol Version 3
ST	Security Target
TOE	Target of Evaluation
TSS	TOE Summary Specification
CAT	Connection Action Table
X.509	Digital Certificate Standard

2 TOE Description

2.1 Overview

CypherNET is a high-speed, standards based multi-protocol encryptor specifically designed to secure voice, data and video information transmitted over Fibre Channel and Ethernet Networks. It can be deployed within Networks employing data rates up to 10 Gigabits per second and provides support for AES algorithms. CypherNET also provides access control facilities using access rules for each defined Ethernet and Fibre Channel connection. Plug in interface cards enable CypherNET to be customised in the field for connection to the required network.

CypherNET 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, CypherNET Ethernet will not discard any valid Ethernet frames for all modes of operation.

CypherNET Fibre Channel connects to Fibre Channel links to provide traffic encryption over point to point (link) network segments. The one interface provides Fibre Channel link encryption at 1, 2, and 4 Gbps to support future network upgrades. 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.

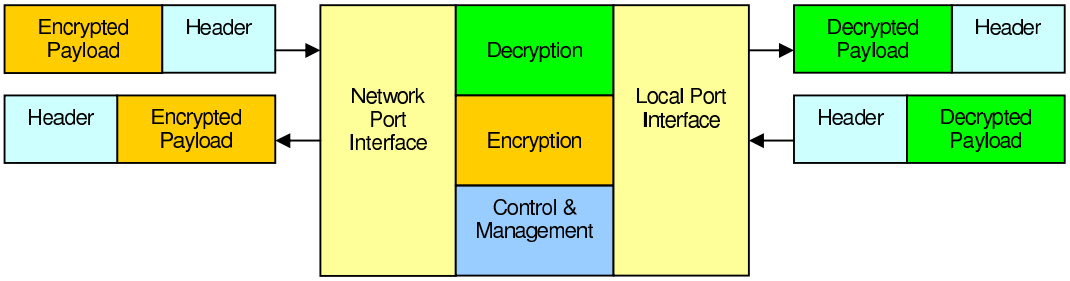

Figure 1 – CypherNET Block Diagram

CypherStream connects to the Local Area Network (LAN) or Wide Area Network (WAN) using 10/100 BaseT RJ45. CypherStream is specifically designed to be a cost-effective solution to interconnect branch and head offices. It is compatible with CypherNET Ethernet encryptors and can operate in both point – point and mesh configurations.

CypherNET and CypherStream 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 CypherNET Ethernet encryptor is shown in Figure 2 and a Fibre Channel encryptor is shown in Figure 3

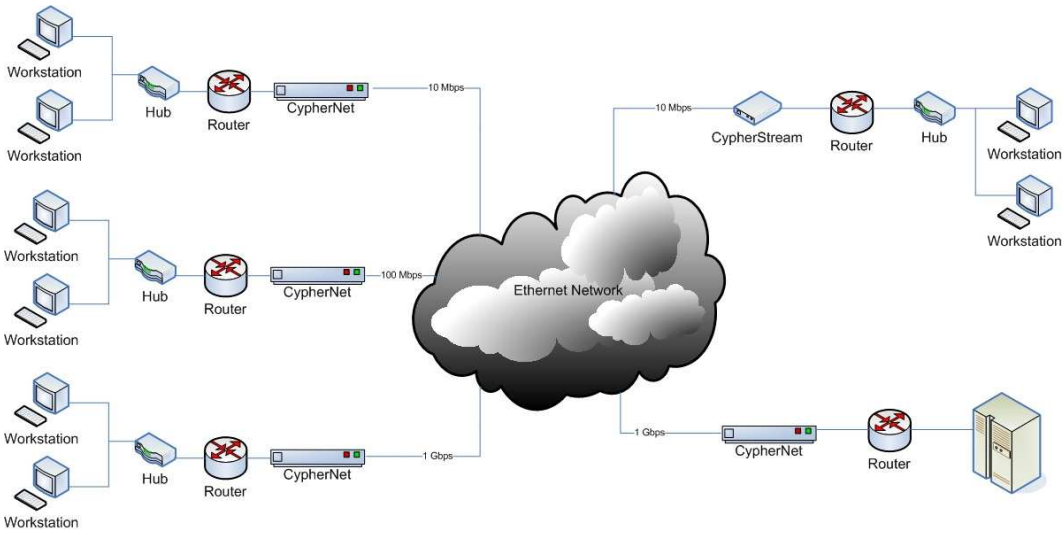

Figure 2 – Ethernet Security Solution

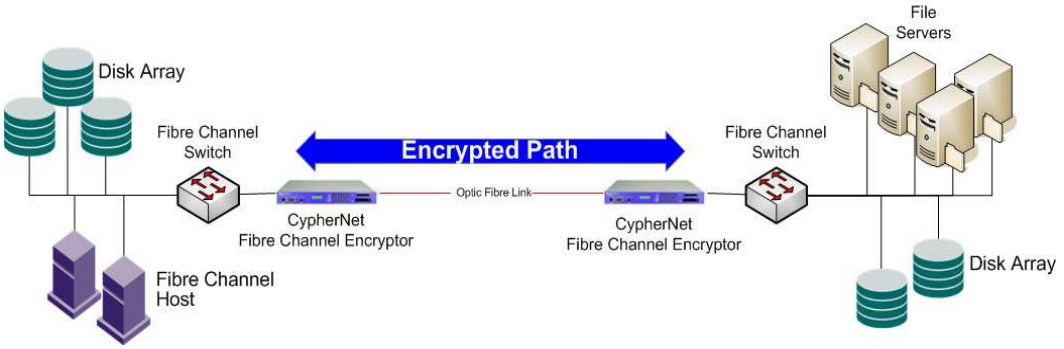

Figure 3 – Fibre Channel Security Solution

CypherNET and CypherStream encryptors can be securely remotely managed by using CypherManager, a SNMPv3 compliant management station. Remote management sessions connect to the encryptor through the dedicated front panel Ethernet port or logically via the local or network interfaces. The encryptors can also be managed locally through the RS232 console port supporting a Command Line Interface (CLI).

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

CypherNET and CypherStream 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 CypherNET or CypherStream encryptor should ensure that an appropriate operational environment is maintained that satisfies those assumptions listed in section 3 of this Security Target.

IdQuantique have developed a quantum key distribution system (QKD) to generate and exchange cryptographic keys over fiber optic networks with absolute security. The QKD keys can be provided to CypherNet encryptors as input into session keys for data encryption. This combination of IdQuantique and CypherNet is known as Cerberis. Although the IdQuantique product is not in the scope of the TOE, the CypherNet encryptor using QKD keys is in scope (the TOE scope is shown below the dotted line in Figure 4).

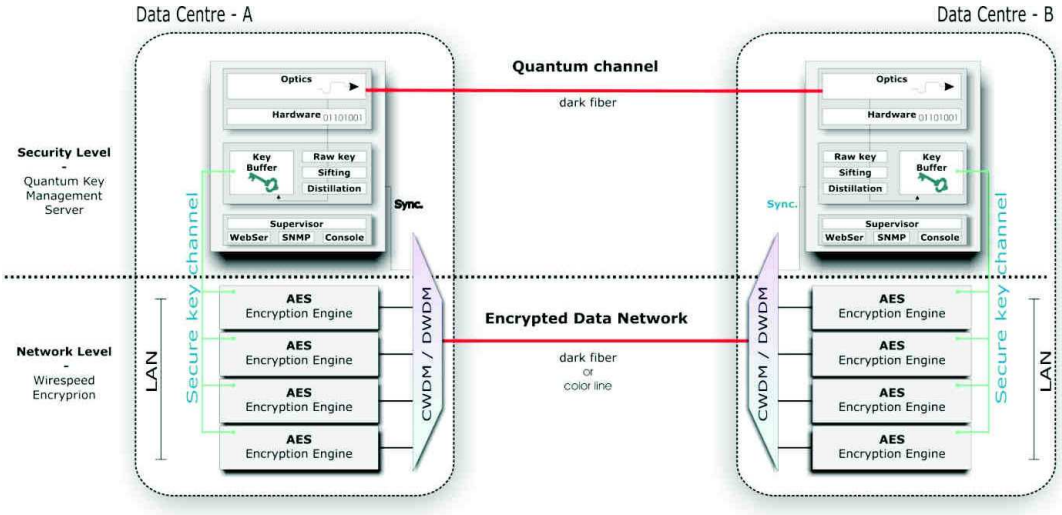

Figure 4 – Cerberis security solution

2.2 Security Features

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

2.2.1 Ethernet Processing

CypherNET and CypherStream 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 5.

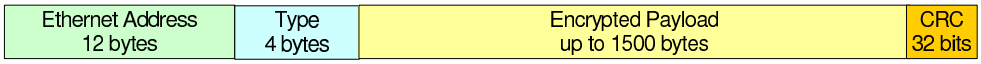

Figure 5 – Ethernet frame format

RSA public key cryptography and X.509 certificates are used to provide a fully automated key management system. Master keys are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. Session keys are transferred periodically between encryptors using master keys.

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

CypherNET and CypherStream provide access control by discarding frames if the access rules for that particular virtual circuit are violated. Access controls may be set for any Ethernet address 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.

2.2.2 Fibre Channel Processing

CypherNET 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.

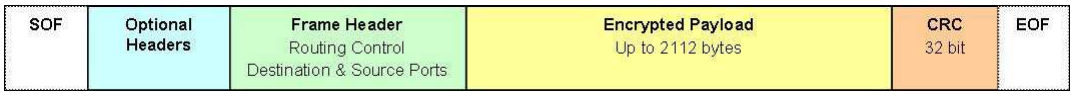

Figure 6– Fibre Channel frame format

RSA public key cryptography and X.509 certificates are used to provide a fully automated key management system. Master keys are transferred between encryptors using X.509 certificate authenticated RSA public key cryptography. Session keys are transferred periodically between encryptors using master keys.

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

2.3 Secure Management

The TOE provides the following secure management features.

2.3.1 Certification Authority

Each encryptor must have an X.509 certificate, which has been signed by CypherManager acting as a Certification Authority (CA), installed before operation of the encryptor can commence.

CypherStream users can access the local management RS232 port to initialise the encryptor with an X.509 certificate; for Cyphernet users, this functionality is restricted to CypherManager using an SNMPv3 management session.

2.3.2 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.

2.3.3 Remote Management using SNMPv3

CypherManager, which uses SNMPv3 management sessions, as well as acting as a CA, provides secure remote management of CypherNET and CypherStream. By default, CypherManager enforces a user to have an authentication password for remote management sessions.

CypherManager, 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 local and network interface ports for in-band management.

2.3.4 Cerberis

Cerberis comprises of at least two devices connected together as shown in Figure 7. The design supports multiple point-to-point links with one or more CypherNET units connected to one QKD unit.

A Senetas CypherNET 1 Gb Ethernet encryptor provides layer 2 network encryption and uses a physically connected QKD as a source of encryption keys; the Key Exchange channel is via a secure RS-232 interface.

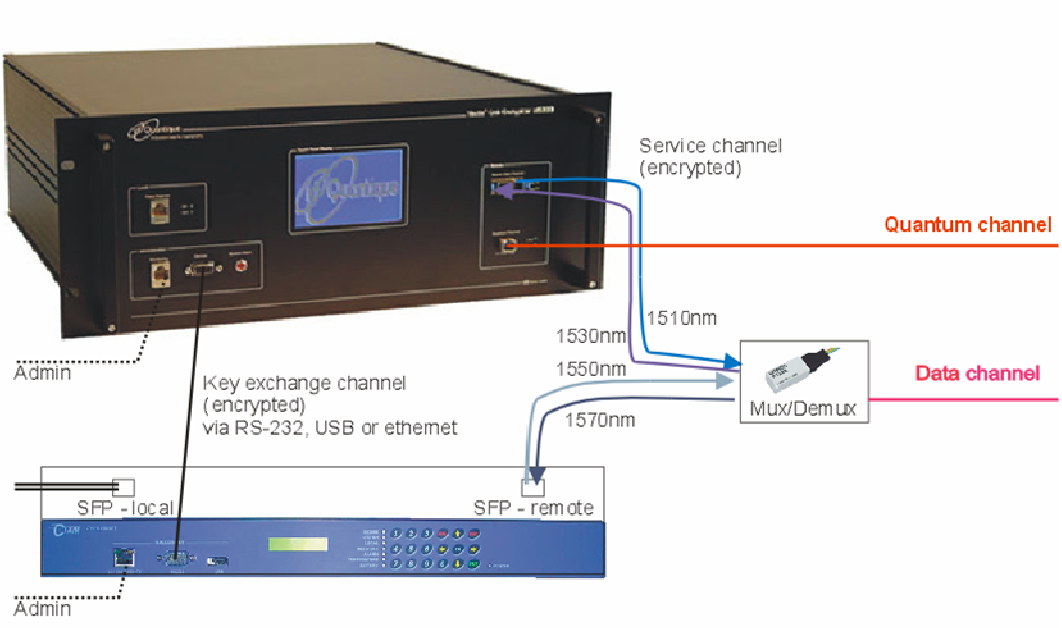

Figure 7 - Cerberis configuration

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 CypherNET, CypherStream and CypherManager apply.

Assumption	Description
Physical Assumptions	
A.CYPHERMANAGER	CypherManager 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. It is assumed that CypherManager will be installed on a computer with the following minimum system configuration: • 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	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.
Personnel Assumptions	
A.ADMIN	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.

Assumption	Description
A.AUDIT	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.
A.PRIVATEKEY	It is assumed that a password used to protect the private key of the CypherManager remote management station is restricted to only Administrators.
Connectivity Assumptions	
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 3shows how to secure a Fibre Channel Link network.
Cerberis Assumptions	
A.CERBERIS	It is assumed that the QKD devices in the Cerberis configuration are installed and managed in a similar manner to the CypherNET encryptors. This includes the same level of physical security and the same trusted personnel that administer the CypherNET encryptors.

Table 5 – 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 an Enhanced-Basic attack potential.

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.

Threat	Description
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.
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, willfully negligent or hostile administrators or other authorised users.

Table 6 – 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	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 Action Table. Any Ethernet frame or Fibre Channel frame for which there is no CAT entry, is discarded. By default, all Ethernet frames and Fibre Channel frames are discarded. 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.ROLES	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). The P.ROLES OSP ensures that administration of the TOE is performed in accordance with the concept of *least privilege*.

Table 7 – 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 8 – TOE Security Objectives

4.2 Environmental Security Objectives

Objective	Description
O.AUDITLOG	Authorised users of the TOE must ensure that audit facilities are used and managed effectively. In particular: 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	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.
O.CONNECT	Those responsible for the TOE must ensure that no connections are provided to outside systems or users that would undermine IT security.
O.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.
O.PERSONNEL	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.
O.PHYSICAL	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.
O.ROLEMGT	The administrator responsible for controlling who has access to the unit for configuration and monitoring activities must allocate users roles with the concept of *least privilege*. There are three roles: Administrator: who has full access rights; Supervisor: who has full access rights except they cannot add, delete or modify user accounts, they cannot install X.509 certificates and they cannot upgrade the firmware; and

	Operator: who can view all available information but cannot delete, add or modify the information
O.CERBERISMGT	The QKD devices in the Cerberis configuration are installed and managed in a similar manner to the CypherNET encryptors. This includes the same level of physical security and the same trusted personnel that administer the CypherNET encryptors.

Table 9 – 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 encrypt the CypherManager private key. 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 – 1024, 2048 and 4096 bits*, that meet the following: *FIPS PUB 186-2 Digital Signature Standard, Appendix 3*.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction
Application note: The Encryptor can now generate 1024 and 2048 bit RSA key sizes. Correspondingly, CypherManager generates 1024, 2048 and 4096 bit RSA key sizes

5.1.2.4 FCS_CKM.1.D – Cryptographic key generation

Hierarchical to: No other components

FCS_CKM.1.1.D The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, *AES* and specified cryptographic key sizes *256 bits* that meet the following: no standard .

Application note: The TOE receives input from the QKD device in the environment which is then XORed with the internally generated key to provide a resultant AES key. XORing the provided input with the internal key ensures the entropy of the resultant session key.

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

5.1.2.5 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 Master/Session key using X.509 certificates for authentication*, that meets the following: *ATM Forum Security Specification V1.1, PKCS #1*

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

5.1.2.6 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: *The session keys used to encrypt the payload of the Ethernet and Fibre Channel frame are held in volatile memory. Loss of electrical power will destroy all session keys. If the case is opened, then the master keys used to encrypt the RSA private key and user passwords are automatically erased* that meets the following: *none*.

Dependencies: FCS_CKM.1 Cryptographic key generation

5.1.2.7 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 CypherManager private key.

5.1.2.8 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) and counter (CTR) mode* 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 FIPS PUB SP800-38A*.

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

5.1.2.9 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 key sizes *1024, 2048, 4096 bits* that meet the following: *ATM Forum Security Specification V1.1, PKCS#1*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
Application note: The Encryptor can now use 1024 and 2048 bit RSA key sizes. Correspondingly, CypherManager can use 1024, 2048 and 4096 bit RSA key sizes.

5.1.2.10 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-1, SHA-256* and cryptographic key sizes *160, 256 bits respectively*, that meet the following: *FIPS PUB 180-1*.

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

5.1.2.11 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 key sizes *1024, 2048 and 4096 bits* that meet the following: *PKCS#1*.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
Application note: The Encryptor can now use 1024 and 2048 bit RSA key sizes. Correspondingly, CypherManager can use 1024, 2048 and 4096 bit RSA key sizes.

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:

- *Channel Action Table;*
- *User Table;*
- *System Time;*
- *Audit Log;*
- *X.509 Certificate; and*
- *Firmware.*

Operations: Management operations, consisting of:

- *Viewing Channel Action Table, User Table, System Time and Audit Log;*
- *Modifying Channel Action Table, User Table and System Time;*
- *Clearing the Audit Log;*
- *Activating X.509 Certificate;*
- *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 users 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 Certificate generation requests from an encryptor and new X.509 Certificates generated by CypherManager 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*
- *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 in the Ethernet header, R_CTL and D_ID field content contained in the Fibre Channel frame header, is listed in the CAT then the defined operation in the CAT is allowed.*

FDP_IFF.1.3 The TSF shall enforce the *additional information flow control SFP rules:*

- *If the operation in the CAT is defined as "encrypt" then the Ethernet frame or Fibre Channel frame will be passed with the Ethernet payload, or Fibre channel payload and a user configurable portion of the header, encrypted/decrypted.*
- *If the operation in the CAT is defined as "bypass" then the Ethernet frame, or Fibre Channel frame will be passed without modification.*
- *If the operation in the CAT 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: FAI_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_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 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 CAT 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*

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 *CAT table, User Account table, X.509 certificate* to *administrators*

- *change_default, query, modify, delete and clear* the *CAT table and query the User Account table* to *supervisors.*
- *query* the *CAT 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 and operator*.

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 EAL4 + 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	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 CypherManager. 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). Authorised users can view the audit log, using SNMPv3 remote management from CypherManager or through the console port. 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 CypherManager and the console mode presenting the data as a scrolled list of audit text. (FAU_SAR.1) 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.

IT Security Function	Security Functional Requirements	Description
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	The TOE shall manage all necessary tasks to support X.509 certificate based authentication. These tasks are: a. Generating and installing signed X.509 certificates into the encryptor b. Authenticating received X.509 certificates using installed trusted CA root certificates Operations relating to generating, X.509 certificates require the use of the RSA algorithm to generate the private and public key pair (FCS_COP.1.1.C). X.509 certificate signing operations are done using the RSA (FCS_COP.1.1.G) signature algorithm. When CypherManager requests a new public key from an encryptor, the encryptor hashes the data that will be returned using SHA-1 (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 CypherNet encryptor, or on the Command Line of the CypherStream encryptor. (FDP_DAU.1.2). CypherManager also hashes the received data and displays the validation code. Both the CypherManager user and the remote operator must agree that the validation codes are the same before the CypherManager user signs the X.509 certificate. When CypherManager returns the signed certificate the same process is repeated again with the CypherManager user and remote operator agreeing that the validation codes are the same before the X.509 certificate is loaded into the encryptor. The Encryptor uses the certificate to establish a trusted communications channel between itself and other Encryptors (remote trusted IT products). Both encryptors must have a valid X.509 certificate, which has been signed by a trusted CA, to protect the confidentiality and integrity of transmitted information and is logically distinct from other channels (FTP_ITC.1).

IT Security Function	Security Functional Requirements	Description
F.DATA_EXCHANGE	FCS_COP.1.1.B FDP_UCT.1.1	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 CAT entry requires encryption of traffic on that address or frame type. If encryption is required, the encryptor performs hardware- or software based 128 or 256 bit AES encryption in CFB or counter mode 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). The various models use the following encryption methods and algorithms (FCS_COP.1.B): • 10/100/1000 Ethernet uses AES with 256 bit key using the self synchronising CFB mode • 10 Gigabit Ethernet uses AES with 256 bit key using counter mode • Fibre Channel uses AES with 256 bit key using the self synchronising CFB mode • CypherStream Ethernet uses AES with 128 or 256 bit key using the self synchronising CFB mode
F.IDENTIFICATION	FIA_AFL.1.1 FIA_AFL.1.2 FIA_UAU.2.1 FIA_UID.2.1	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. All user passwords must have a minimum length of eight characters. The set of possible characters are A-Z, a-z, 0-9 and ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] : ; ” ’ , < . > ? / |\. For local 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

IT Security Function	Security Functional Requirements	Description
		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. For remote management using SNMPv3 the CypherManager 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 CypherManager 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 CypherManager 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 identified and authenticated in this way.

IT Security Function	Security Functional Requirements	Description
F.KEY_ MANAGEMENT	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	The TOE shall manage all the necessary keys and mechanisms to support its cryptographic operations, namely: a. Generating RSA public/private key pairs for both CypherManager and encryptors. (FCS_CKM.1.1.C) b. Generating and securely transferring master keys 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 (FCS_CKM.2.1.A); c. Updating session keys used for AES encryption between encryptors. (FCS_CKM.2.1.A) AES session keys 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 master CSP 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. Session keys 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	The TOE shall control the flow of Ethernet frames or Fibre frames received on the private network interface and on the public network interface from external hosts 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 (FDP_IFC.1, FDP_IFF.1.1). 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). The TOE determines the appropriate action to take on any given frame by examining the list of entries in the CAT. By default, for a given address that is not listed in the CAT, the frame is discarded (FDP_IFC.1, FDP_IFF.1.1). The CAT 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 CAT to override the default values (FMT_MSA.3.A).
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	The TOE can be accessed and managed using SNMPv3 packets received on the Ethernet management port interface and the local and network interfaces or via the console management port interface. The encryptor's USB port can be used to upgrade firmware (FDP_ACC.1). 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: Administrators: Who can change defaults, query, modify, delete and clear the CAT

IT Security Function	Security Functional Requirements	Description
		and the CAT information flow address and actions (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). Supervisors: Who can change defaults, query, modify, delete and clear the CAT (FMT_MSA.1.1.A), view the User accounts table and audit log and set the system time (FMT_MSA.1.B). Operators: Who can query the CAT and User Account tables only, and view the audit log. When the TOE is accessed the TOE associates users with these roles and prevents a user from performing operations on the TSF's that they are not authorised to perform (FMT_SMR.1). 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). 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)

IT Security Function	Security Functional Requirements	Description
F.SECURE_ REMOTE_ MANAGEMENT	FPT_ITT.1.1 FCS_COP.1.1.B	The TOE shall protect the confidentiality of remote management data between the encryptors and the CypherManager remote management station. (FPT_ITT.1) 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) The user initiates the remote management session by executing the CypherManager software on their workstation.
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	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 master key is erased from battery-backed volatile memory (FCS_CKM.4). The master key encrypts all private key material and user password data, and so removal of the master key means the encrypted data cannot be accessed. 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). The TOE protects its own private key on CypherManager 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 CypherManager.

IT Security Function	Security Functional Requirements	Description
F.CERBERIS	FCS_CKM.1.1.D	In the Cerberis configuration the CypherNET encryptor receives session key input from a QKD device via the RS-232 serial port. The input is combined (XORed) with the internally generated key value to generate a composite session key used for AES 256 data encryption (FCS_CKM.1.D). XORing the input with the internal key ensures the entropy of the resultant session key. This session key is then treated the same as the other session keys in that it is updated according to schedule and is deleted when the encryptor power is removed.

Table 10 – 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 / Assumptions, Threats, OSPs	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	O.CERBERISMGT
ASSUMPTIONS																			
A.ADMIN													✔						
A.AUDIT			✔																
A.CYPHERMANAGER											✔			✔					
A.INSTALL											✔								
A.LOCATE											✔			✔					
A.PRIVATEKEY				✔															
A.CERBERIS																			✔
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 11 – 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	*O.PERSONNEL* ensures that only trusted and competent administrators are authorised to manage the TOE.
A.AUDIT	*O.AUDITLOG* ensures that the facilities to effectively manage audit information are provided.
A.CYPHERMANAGER	*O.INSTALL* ensures that the CypherManager Management Station is installed and managed in a secure environment. *O.PHYSICAL* ensures that the CypherManager Management Station will be protected from physical attacks The combination of these objectives will prevent unauthorised users from attempting to compromise the security functions of the CypherManager Management Station and therefore cover this assumption.
A.INSTALL	*O.INSTALL* ensures that the TOE is delivered, installed, managed and operated in a manner that maintains security.
A.LOCATE	*O.INSTALL* ensures that encryptors are installed correctly in a secure environment while *O.PHYSICAL* ensures that this environment remains secure from unauthorised people.
A.PRIVATEKEY	*O.AUTHDATA* 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 CypherManager's private key.
A.CERBERIS	*O.CERBERISMGT* ensures that any QKD devices in the environment are installed and managed in a similar manner to the CypherNET encryptors. This includes the same level of physical security and the same trusted personnel that administer the CypherNET encryptors.

Table 12 – Informal argument of assumptions

7.1.2.2 Threats

Threat	Justification

Threat	Justification
T.ABUSE	*O.AUDIT* provides a means of recording security relevant events and *O.AUDITLOG* ensures that the facilities to effectively manage audit information are provided. This allows authorised users to detect modifications. This will prevent compromises being undetected. *O.ROLES* ensures the user can only access the operations that the role authorises. *O.ROLEMGT* ensures that users are allocated roles with *least privilege*. This can minimise the threat damage caused by the role. *O.IDENT* ensures that all users are uniquely identified and authenticated before access to TOE management features is allowed. *O.AUTHDATA* 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 (*O.AUDIT* and *O.AUDITLOG*) will deter users from intentionally abusing their privileges. *O.PERSONNEL* 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. The combination of these objectives will reduce this threat to an acceptable level.

Threat	Justification
T.ATTACK	*O.AUDIT* provides a means of recording security relevant events and *O.AUDITLOG* ensures that the facilities to effectively manage audit information are provided. This allows authorised users to detect modifications. This will prevent compromises being undetected. *O.ROLES* ensures the user can only access the operations that the role authorises. *O.ROLEMGT* ensures that users are allocated roles with *least privilege*. This prevents insider users from doing operations for which they are not authorised. *O.ADMIN* ensures that only authorised users can access the TOE management functions. This prevents outsider attackers from accessing the TOE management functions and compromising information. *O.FAILSAFE* 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. The combination of these objectives is sufficient to reduce undetected logical attacks from insiders and outsiders to an acceptable level.
T.CAPTURE	*O.INFOFLOW* 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. *O.ENCRYPT* 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. *O.KEYMAN* ensures the session keys used to encrypt the payloads for *O.ENCRYPT* are kept private by using secure key generation, distribution, agreement, encryption, destruction and exchange techniques. When these objectives are met, the threat of confidential information being recovered by an attacker will suitably diminish.

Threat	Justification
T.CONNECT	*O.INFOFLOW* 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. *O.KEYMAN* 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. *O.CERTGEN* supports *O.KEYMAN* by ensuring the TOE has the capability to generate, issue and manage X.509 certificates. *O.CONNECT* supports the environment to ensure that connections that would undermine security are not established by those responsible for the TOE. When all these objectives are met, the threat of an insecure connection being created by an attacker will be suitably diminished.
T.IMPERSON	*O.IDENT* 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 *O.AUTHDATA* ensures that users are responsible not to disclose their authentication data so attackers cannot impersonate authorised users. *O.ADMIN* ensures only authorised users can manage the TOE and its security features. *O.AUDIT* provides a means of recording security relevant events and *O.AUDITLOG* 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. When all these objectives are met, the threat of privileged users being impersonated by an inside or outside attacker will suitably diminish.

Threat	Justification
T.LINK	*O.INFOFLOW* allows authorised users to explicitly allow connections, however, by default, all connections to the TOE will be discarded. *O.ENCRYPT* allows for the encryption of Ethernet and Fibre Channel payloads. *O.KEYMAN* provides the means for exchanging keys with only other authorised encryptors to establish a link. The other encryptors are only authorised due to X.509 certificate attributes as provided by *O.CERTGEN*. So *O.KEYMAN* and *O.CERTGEN* restrict the number of possible communications paths to only other authorised encryptors. The objectives *O.INFOFLOW, O.KEYMAN* and *O.CERTGEN* combine to minimise the number of communication links that an encryptor will have. The minimal links will reduce the opportunity an attacker has to deduce information. As confidential information over these links will be encrypted due to *O.ENCRYPT*, the attacker will require more resources and knowledge to deduce any useful information. Therefore the combination of all these objectives will lower this threat to an acceptable level.
T.MAL	*O.FAILSAFE* ensures that the TOE will enter a secure state if any malfunction of the TOE is detected.
T.OBSERVE	*O.REMOTEMGT* 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 session keys. *O.KEYMAN* supports *O.REMOTEMGT* to allow cryptographic key management to enable cryptographic exchanges between the encryptor and CypherManager. When all these objectives are met, the threat of legitimate management communications being observed by an attacker will be suitably diminished.

Threat	Justification
T.PHYSICAL	*O.INSTALL* ensures that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security. *O.PHYSICAL* ensures that those parts of the TOE that are critical to security policy enforcement are protected from physical attack. *O.PERSONNEL* ensures that those responsible for the TOE are competent to manage the TOE and can be trusted not to deliberately abuse their privileges. The above environmental objectives provide a secure environment for the TOE to reduce a physical attack from occurring. *O.TAMPER* 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. With all objectives met, this threat is removed.
T.PRIVILEGE	*O.ROLES* ensures the user can only access the operations that the role authorises. *O.ROLEMGT* ensures that users are allocated roles with *least privilege*. This limits the operations and therefore the damage a compromise can lead to. *O.PERSONNEL* ensures that users within the environment are trusted and competent. This will minimise the threats from hostile or wilfully negligent administrators. *O.IDENT* ensures that a user requesting information is correctly identified. While *O.AUTHDATA* 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. *O.AUDIT* provides a means of recording security relevant events and *O.AUDITLOG* 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 *O.IDENT* will be recorded in the audit log, so privileged users will have their actions recorded and reviewed to deter them from abusing their privileges. When all these objectives are met, the threat of privileged users compromising information is suitably diminished.

Table 13 – Informal argument of threats

7.1.2.3 Policies

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

Table 14 – Informal argument of policies

7.1.2.4 Rationale

Given the arguments in the above tables and the mapping's shown in Table 11, 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.1.1.D								✔			
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						✔					

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
FDP_UCT.1.1				✔							
FIA_AFL.1.1							✔				
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 15 – 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	*FDP_ACC.1.1*, *FDP_ACF.1.1*, *FDP_ACF.1.2*, *FDP_ACF.1.3* and *FDP_ACF.1.4* 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 *O.ADMIN*. *FTA_SSL.3.1* provide additional protection, automatically terminating management sessions after a period of user inactivity. *FMT_MTD.1.1* provides the function so authorised roles can manage the TSF data. *FMT_SMF.1.1* provides security management of attributes and data to allow administration of the TOE.
O.AUDIT	FAU_GEN.1.1 FAU_GEN.1.2 FAU_SAR.1.1 FAU_SAR.1.2 FPT_STM.1.1	*FAU_GEN.1.1* and *FAU_GEN.1.2* provide the capability for generating and recording audit events in the manner required by *O.AUDIT*. *FAU_SAR.1.1* and *FAU_SAR.1.2* provide the capability for viewing audit logs to support the effective use and management of the audit facilities in a manner required by *O.AUDIT*. *FPT_STM.1.1* ensures that a date and time stamp is recorded with the audit record.

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	*FCS_COP.1.1.C* uses the RSA algorithm to encrypt the RSA private key for X.509 certificates. *FCS_COP.1.1.G* together with *FCS_COP.1.1.F* 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. *FDP_DAU.1.1* and *FDP_DAU.1.2* provides the means for producing a digest of the data for authentication purposes, when generating partial X.509 certificates in certificate load mode, and after sending completed and signed X.509 certificates from CypherManager to the encryptor. *FTP_ITC.1.1, FTP_ITC.1.2* and *FTP_ITC.1.3* provides the means for using the X.509 certificates to authenticate other encryptors and establish a secure trusted channel.
O.ENCRYPT	FCS_COP.1.1.B FDP_UCT.1.1	*FCS_COP.1.1.B and FDP_UCT.1.1*, 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. The cryptographic functions meet the standards required by FIPS 140-2 and ISM.
O.FAILSAFE	FPT_FLS.1.1 FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3	*FPT_FLS.1.1* together with *FPT_TST.1.1, FPT_TST.1.2* and *FPT_TST.1.3* 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.

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	*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* and *FMT_MSA.3.2.A* together provide the capability for authorised users to control traffic flow between subjects using the Ethernet MAC address or the contents of the R_CTL and D_ID fields in the Fibre Channel frame in a manner required by O.INFOFLOW.
O.IDENT	FIA_UAU.2.1 FIA_UID.2.1 FIA_AFL.1.1 FIA_AFL.1.2	*FIA_UAU.2.1* and *FIA_UID.2.1* provide the capability for identifying and authenticating all users in a manner required by O.IDENT. *FIA_AFL.1.1* and *FIA_AFL.1.2* provide additional protection by limiting the number of unsuccessful authentication attempts before imposing a timeout on that user account.
O.KEYMAN	FCS_COP.1.1.C FCS_CKM.1.1.A FCS_CKM.1.1.B FCS_CKM.1.1.C FCS_CKM.1.1.D FCS_CKM.2.1.A FCS_CKM.4.1	*FCS_CKM.1.1.A, FCS_CKM.1.1.B, FCS_CKM.1.1.C, FCS_CKM.1.1.D, FCS_CKM.2.1.A,* and *FCS_CKM.4.1* 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. *FCS_COP.1.1.C* provides RSA encryption of session keys. These cryptographic functions meet the standards required by FIPS 140-2 and ISM. *FCS_CKM.1.1.D* provides the functionality for the encryptor to receive cryptographic key input from the QKD device in order to generate AES 256 bit keys. The QKD provided input is XORed with the internally generated key to ensure the entropy of the resultant AES session key.

Objective	Security Functional Requirement	Justification
O.REMOTEMGT	FCS_COP.1.1.B FPT_ITT.1.1	*FCS_COP.1.1.B,* provides the capability for encryption methods for management data over the network. *FPT_ITT.1.1* ensures the confidentiality of remote management information is maintained.
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	*FMT_SMR.1.1* specifies the three possible roles administrator, supervisor and operator. *FMT_MSA.1.1.B, FMT_MSA.3.1.B, FMT_MSA.3.2.B* defines each role's privileges for managing the TSF security attributes. *FMT_MTD.1.1* defines each role's privileges for managing the TSF data. *FMT_SMR.1.2* associates a human with one role. In combination, these SFRs restricts the human's access to only those TSF attributes, data and operations explicitly allowed by the associated role.
O.TAMPER	FPT_PHP.3.1.A FPT_PHP.3.1.B FCS_COP.1.1.A FCS_CKM.4.1	*FPT_PHP.3.1.A and FPT_PHP.3.1.B* 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. *FCS_COP.1.1.A* provides the capability for the TOE to encrypt the private keys and user passwords using 3DES. *FCS_CKM.4.1* provides the capability to delete the Master key by disconnection of battery as key is held in battery-backed volatile memory.

Table 16 – Informal Argument of Sufficiency

Given the arguments in Table 16 and the mappings shown in Table 15, it has been demonstrated that the security functional requirements are sufficient to enforce the security objectives for the TOE.

7.2.3 Rationale for EAL4 + ALC_FLR.2 Assurance Level

In Part 3 of the CC EAL4 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.

EAL4 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 4 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.

End