Security Target for Common Criteria Evaluation:

Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager

February 26, 2009

Document Reference: ST

Document Version 1.9

Document Introduction

Prepared For:

Thales e-Security, Inc.
2200 North Commerce Parkway, Suite 200
Weston, Florida 33326
www.thales-esecurity.com

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive, Ste. 101
Apex, NC 27502
www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Figures

List of Tables

Acronyms List

AES.....**Advanced Encryption Standard**
ANSI.....**American National Standards Institute**
CA.....**Certificate Authority**
CAVP.....**Crytpographic Algorithm Validation Program**
CBC.....**Cipher Block Chaining**
CC.....**Common Criteria**
DEK.....**Data Encryption Key**
DH ESK.....**Diffie-Hellman Encrypted Secret Key**
DSS.....**Digital Signature Standard**
EAL.....**Evaluation Assurance Level**
FIPS.....**Federal Information Processing Standard**
GUI.....**Graphical User Interface**
HMAC.....**Hashed Message Authentication Code**
IT.....**Information Technology**
ITU.....**International Telecommunications Unit**
KEK.....**Key Encryption Key**
LAN.....**Local Area Network**
NIAP.....**National Information Assurance Partnership**
OC.....**Optical Carrier**
PP.....**Protection Profile**
RFC.....**Request for Comment**
RIP.....**Routing Information Protocol**
RTC.....**Real Time Clock**
SDH.....**Syncronous Digital Hierarchy**
SHA.....**Secure Hashing Algorithm**
SHS.....**Secure Hashing Standard**
SF.....**Security Function**
SFP.....**Security Function Policy**
SOF.....**Strength of Function**
SONET.....**Syncronous Optical NETwork**
SPE.....**Synchronous Payload Envelope**
ST.....**Security Target**
TOE.....**Target of Evaluation**
TSC.....**TSF Scope of Control**
TSF.....**TOE Security Function**
TSFI.....**TSF Interface**
TSP.....**TOE Security Policy**
VC.....**Virtual Container**
WAN.....**Wide Area Network**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Target of Evaluation is the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Document Title:	Security Target for Common Criteria Evaluation: Thales e-Security Datacryptor SONET/SDH and Gigabit Ethernet with Element Manager
Document Version:	1.9
Date of Release:	February 26, 2009

1.2 TOE Reference

The Target of Evaluation is the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL3 (Evaluation Assurance Level 3) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.4 Keywords

The following keywords are applicable to the TOE: Layer 2 Encryption, Optical Networking, SONET, SDH, Gigabit Ethernet.

1.5 TOE Overview

This Security Target defines the requirements for the Thales e-Security Datacryptor SONET/SDH Release 4.0 with Element Manager and Thales e-Security Datacryptor Gigabit Ethernet Release 4.0 with Element Manager.

The Datacryptor SONET/SDH provides point-to-point encryption to another Datacryptor over untrusted networks. Each TOE includes Element Manager, which is a GUI application for management and configuration of the Datacryptor SONET/SDH device via the 10/100 Ethernet Management port. Each TOE provides strong encryption at Layer 2, robust key management, detailed auditing, and comprehensive management capabilities to provide security for the most demanding service requirements.

1.6 Security Target Organization

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.7 Common Criteria Conformance

The TOE is compliant with the Common Criteria (CC) Version 2.3, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL3.

1.8 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

1.9 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 SONET/SDH Technology Overview

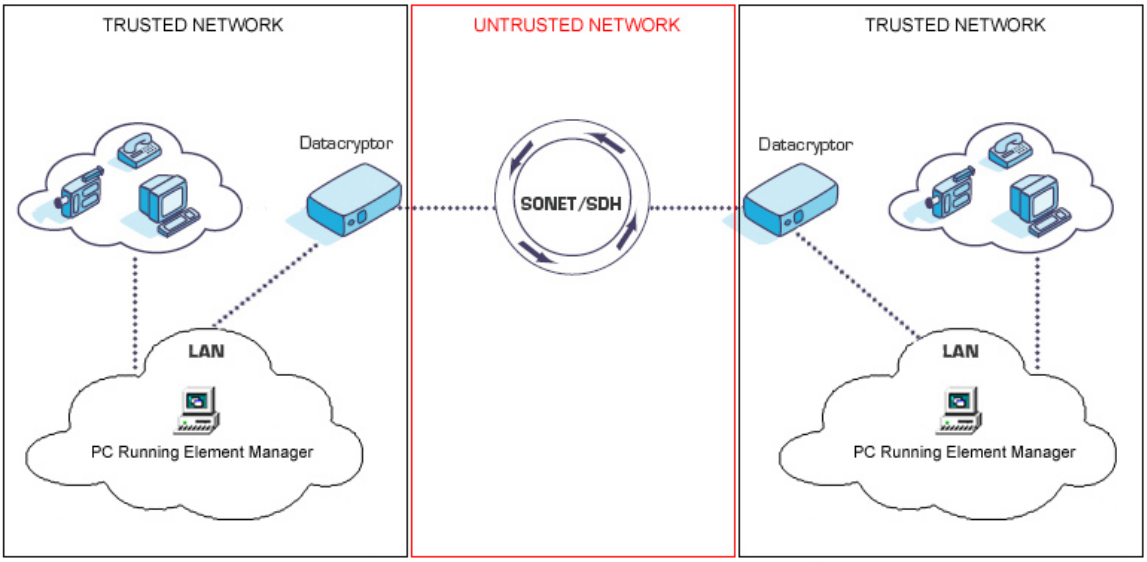
SONET/SDH is a transmission technology for fibre optic telecommunications. The SONET standard was originally developed as an American National Standards Institute (ANSI) specification. The standard was internationalized as SDH by the Consultative Committee on International Telegraphy and Telephony (CCITT), now the International Telecommunications Union (ITU). While native SONET and SDH are very similar, there are a number of structural differences between the protocols used by each standard, including the manner by which the Synchronous Payload Envelopes (SPEs) in SONET and the Virtual Containers (VCs) in SDH are constructed, as well as a number of differences in their respective header characteristics[1].

2.2 Datacryptor SONET/SDH Description

The Thales Datacryptor SONET/SDH implements security features for data flows over a Synchronous Optical Network (SONET). The primary security function of the TOE is to provide confidentiality services for data flows over optical networks, and the other functions of the TOE support this primary function. The TOE is deployed at the edge of an untrusted optical network with the intent to provide secure communications between two trusted networks that are physically separated.

[1] Recognizing these differences, it is important to note that from an encryption perspective, the Datacryptor SONET/SDH is transparent to these differing characteristics.

Figure 1 – SONET/SDH Datacryptors in a Network



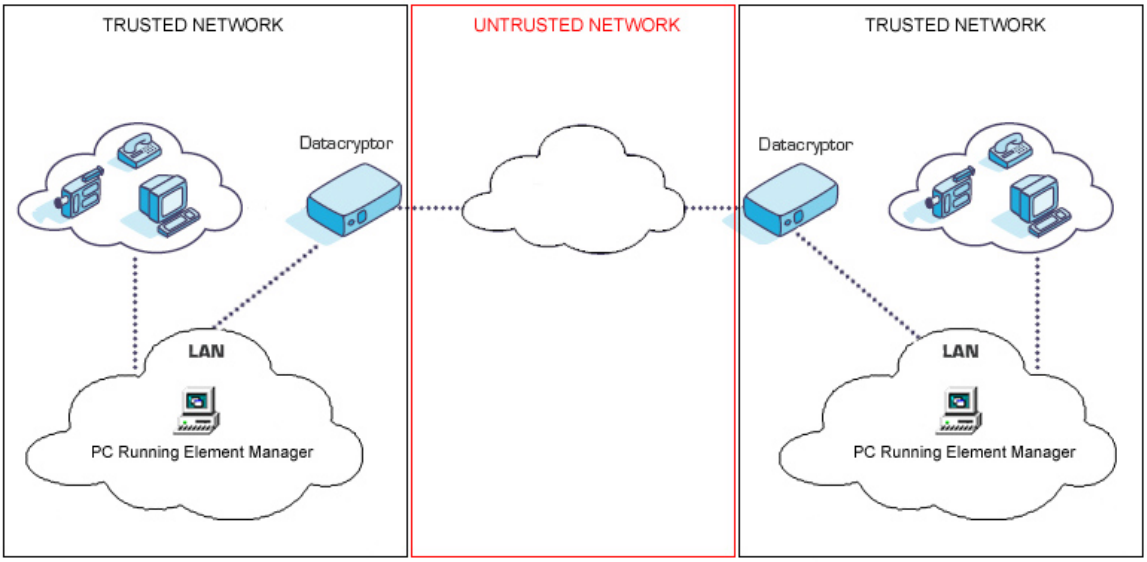
Potential areas of application include scenarios where distant PBX devices, routers (POS) or switches are connected via SONET/SDH links vulnerable to interception and alteration. The Datacryptor SONET/SDH encryption appliance delivers high performance and confidentiality to these usage applications.

The TOE encrypts unencrypted data flows that enter the device from the trusted network side before they are forwarded across the untrusted optical network. When the encrypted data flow reaches the remote device, the TOE decrypts the data before forwarding it to the remote trusted network. In short, data is encrypted at one device's outbound interface and decrypted at the other device's inbound interface.

2.3 Datacryptor Gigabit Ethernet Description

The Thales Datacryptor Gigabit Ethernet implements security features for data flows over an Ethernet network. The primary security function of the TOE is to provide confidentiality services for data flows over untrusted networks, and the other functions of the TOE support this primary function. The TOE is deployed at the edge of an untrusted network with the intent to provide secure communications between two trusted networks that are physically separated.

Figure 2 – Gigabit Ethernet Datacryptors in a Network



The TOE encrypts unencrypted data flows that enter the device from the trusted network side before they are forwarded across the untrusted network. When the encrypted data flow reaches the remote device, the TOE decrypts the data before forwarding it to the remote trusted network. In short, data is encrypted at one device's outbound interface and decrypted at the other device's inbound interface.

2.3.1 TOE Physical Boundary

Each TOE is comprised of two subsystems, the Datacryptor subsystem and the Element Manger subsystem. The former is an appliance that sends, receives, and processes plaintext and encrypted traffic for transmission to a secure network or over an untrusted network. The latter is a GUI management application that is used to configure the Datacryptor. The TOE does not include the operating system hosting the Element Manager, the trusted network, or the untrusted network.

For the Datacryptor subsystem, the physical boundary is the Datacryptor SONET/SDH and Datacryptor Gigabit Ethernet itself. The TOE is completely self-contained; it contains all software and hardware required to perform all security functions. The TOE operating system controls all data encryption and management functions.

The following SONET/SDH hardware models are included in the evaluation:

- OC-3 SONET/SDH
- OC-12 SONET/SDH
- OC-48 SONET/SDH
- OC-192 SONET/SDH

The following Gigabit Ethernet hardware models are included in the evaluation:

- 1 Gigabit Ethernet
- 10 Gigabit Ethernet

Figure 3 - Thales Datacryptor SONET/SDH

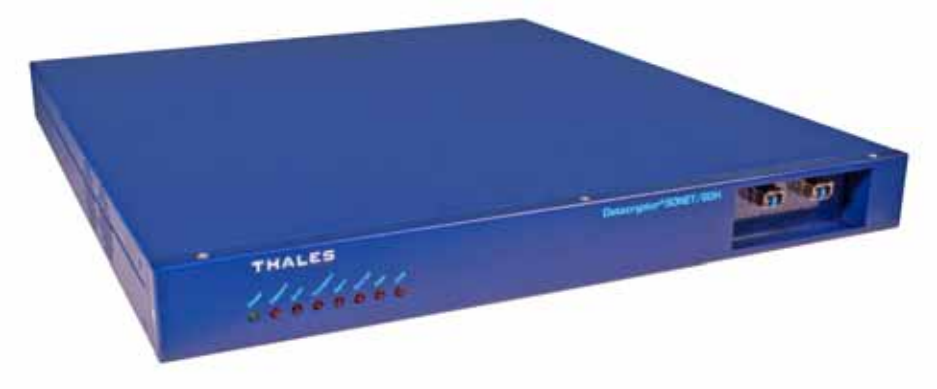
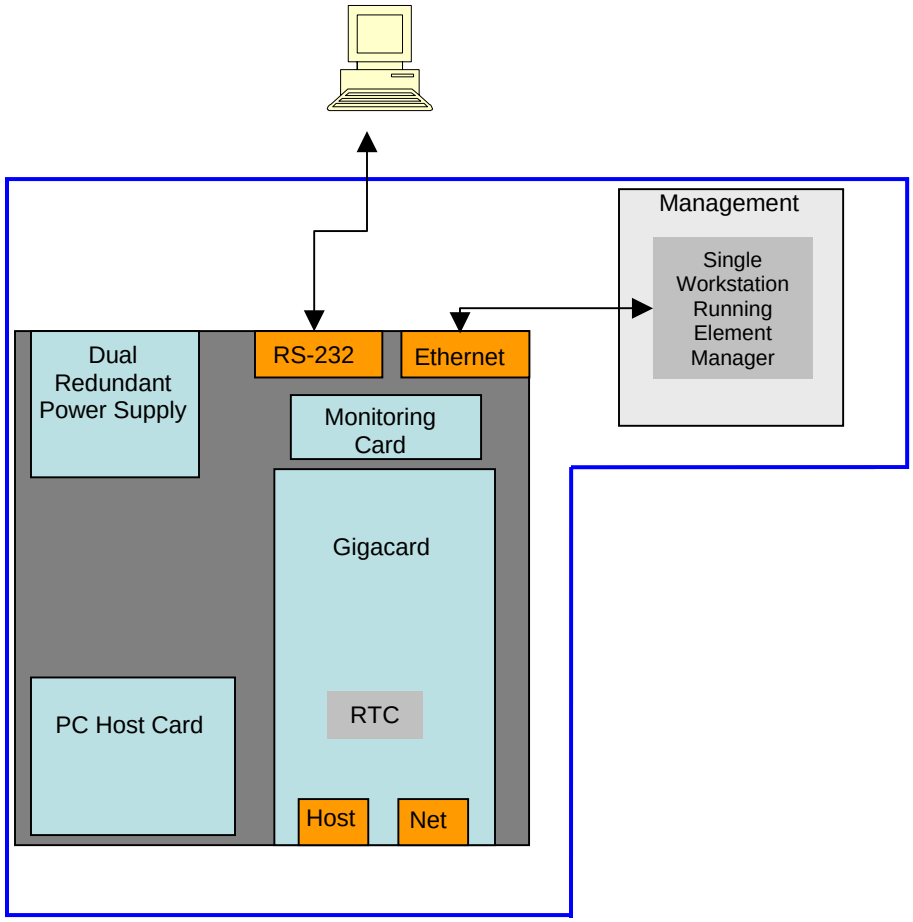


Figure 4 - Thales Datacryptor Gigabit Ethernet

Figure 5 – TOE Physical Boundary



The interfaces to the Datacryptor are highlighted in orange in Figure 2 and include the network interfaces (Host and Net) as well as the management interfaces (RS-232 and Ethernet). The network interfaces pass plaintext and/or encrypted traffic as defined by the configuration, and the management interfaces are used solely for the administration of the Datacryptor SONET/SDH. A brief description of each security-relevant interface follows:

- RS-232 Serial Interface – initial set-up of the unit from a PC hosted Management Interface.
- Ethernet Management – general management of the unit from a PC hosted Management Interface. All management services occur only through this interface via UDP/IP protocol.

- Host – input and output of plaintext (from/to trusted network) traffic. This occurs over the Ethernet protocol for the Gigabit Ethernet Datacryptor and over the SONET protocol for the SONET/SDH Datacryptor[2].
- Net – input and output of ciphertext (from/to untrusted optical network) traffic.

The larger component blocks are described as follows:

- Dual Redundant Power Supply – supplies power to the unit from either 115v/240c AC or 48v DC options.
- Monitoring Card – Monitors internal fans speeds and temperature.
- PC Host Card – Converts high-level control and status commands received from the GigaCard into low level commands for the interface controller.
- GigaCard – Performs all security functionality (including line encryption/decryption and remote management) of the unit and controls the HOST/NET interfaces.

As mentioned above, the Datacryptor has two network interfaces. When the TOE is in use, one of the network interfaces will be connected to a trusted network, and the other interface will be attached to an untrusted network. The TOE configuration will determine how data flows received on one interface will be transmitted on another. Typically, for data flows that are to be protected by the TOE security functions, frame flows received on trusted network interfaces will be encrypted before being transmitted out an untrusted interface.

The following components are outside of the TOE Boundary:

- Single Workstation Running SNMP – this workstation is used only for viewing of basic status and configuration via SNMP. The TOE cannot be configured or managed via SNMP. As such, this component is outside the TOE boundary and is not used in the evaluated configuration of the TOE (see Section 2.4 – Evaluated Configuration).
- Single Workstation Running Certificate Manager – this workstation is used in the initial provisioning process of a Datacryptor and generates Certificate Authority data, which can be backed up to removable media. The Certificate Manager does not connect directly to the TOE.
- Removable Media for Storage of Key Material – the removable media stores Certificate Authority data provided by the Certificate Manager. This data imported by Element Manager and is used for initial provisioning of the Datacryptor; its functionality is not part of normal runtime operations of the TOE in evaluated configuration.

[2] Note that management via Element Manager is not possible over the Host interface as this interface does not allow connections via UDP/IP.

2.3.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

At a high level, the logical boundaries of the TOE are the functions of the TOE interfaces, including audit of security functions, authentication for the administrative functions, the management of the security configurations, controlling the flow of plaintext/ciphertext information, and the self-protection of the TOE itself.

2.3.2.1 Authentication

The TOE (via Element Manger) supports authentication of an authorized administrator, who manages the TOE locally or remotely. The administrator is required to authenticate via password before configuring TOE security functions. The password is used to decrypt various parameters used to verify authentication and encrypt the link between the Element Manager subsystem and the Datacryptor subsystem.

2.3.2.2 Security Audit

The TOE provides one log that reports management operations and errors. This log is stored in the Datacryptor and is viewed by an administrator via Element Manager.

2.3.2.3 Information Flow Control

The TOE provides encryption for data traversing from the trusted network to a remote trusted network, and each Datacryptor allows traffic to flow between subjects (e.g., instances of the TOE connected via an untrusted network and IT Systems connected via the trusted network). The configuration for this data encryption is specified in an Information Flow Control policy.

2.3.2.4 Security Management

The TOE is managed via GUI interface called Element Manager, which interfaces with the Datacryptor via the Ethernet interface. The TOE provides an administrators with the capabilities to configure, monitor and manage the TOE to fulfill the security objectives if the TOE. Security Management principles relate to Security Audit, Information Flow Control, and Cryptographic Support.

2.3.2.5 Protection of Security Functions

The TOE provides various protection mechanisms for its security functions, the enforcement of the information flow control policy and authentication rules at the applicable interfaces. The TOE also ensures that the TSF is protected against interference and tampering by untrusted subjects.

2.3.3 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data

enables the TOE to identify and authenticate users. User Data is information stored in TOE resources that can be operated upon by users in accordance with the TSP and upon which the TSF places no special meaning.

Subjects are the Administrator, IT systems on the LAN, and instances of the TOE on the WAN sides that transmit traffic to the TOE to be forwarded to the other network. The network traffic represents information of which TOE controls the flow.

The following table addresses and categorizes the data present in the TOE:

Table 1 - TOE Data

Name	Description	AD	UA	SA	IA	GC
CA Public Key Component	The Public key of the CA key pair is stored in the Datacryptor® SONET/SDH and is never exported.					✓
Certificate Lifetime	Specifies the dates for which the Certificate is valid. Configured via Element Manager					✓
Data Encryption Key (DEK) for Transmit and Receive	The DEK is used for encrypting and decrypting data traffic.			✓		
DEK Lifetime	Defines validity period for the DEK					✓
KEK Lifetime	Defines validity period for the KEK					✓
Key Encryption Key (KEK)	The KEK is derived and exchanged between TOEs using Diffie-Hellman key agreement. The KEK will encrypt the DEK for secure distribution.			✓		
Password	The password enables the TOE to either authenticate, or fail to authenticate, an administrator.	✓				
Receiving/transmitting interface	Specifies HOST interface for plaintext receipt/transmission over a trusted network or LINE interface for ciphertext receipt/transmission over an untrusted interface			✓		
System date/time settings	The system date and time settings enable the TOE to make decisions about timeout and re-keying. Without time settings, the TOE cannot determine how to perform connection timeouts and re-keying intervals.					✓
Transmission Mode	Specifies Line Mode 1 for encryption of most of the header information and all of the payload or Line Mode 2 for encryption of only the payload.					✓
X.509v1 Certificates and key pair	A Datacryptor generates its own X.509 User Certificates and corresponding Diffie-Hellman key pairs.			✓		

Name	Description	AD	UA	SA	IA	GC
X.509v1 and X.509v3 Certificates for Peer for data integrity	During the first stages of link establishment between two modules they exchange certificates and authenticate each other using signature verification. Once received, these peer Certificates are stored within the module, which reduces overheads for any subsequent link establishment.			✓		

Legend: AD=Authentication data; UA=User attribute; SA=Subject attribute; IA=Information attribute; GC=Generic Configuration Information

2.3.4 Rationale for Non-Bypassability and Separation

2.3.4.1 Datacryptor Subsystem

The Datacryptor subsystem is a stand-alone system that includes all hardware and software required for operation. It is not a general-purpose platform; it is a specialized platform with strictly controlled functionality made available to the users. By limiting the functionality, the TSF is protected from corruption or compromise.

2.3.4.2 Element Manager Subsystem

The Element Manager subsystem is an application that executes on top of an underlying system that includes hardware and software required for operation. Therefore responsibility for non-bypassability and separation are split between the TOE and IT Environment. The TOE provides strictly controlled functionality to the users within the TSC. By limiting the functionality, the TSF is protected from corruption or compromise from users within the TSC. Only a single administrator role is supported.

The IT Environment provides a unique domain for the Element Manager application via the Operating System. And since workstation must be dedicated to running Element Manager, other applications cannot interfere with the interfaces of the Element Manager domain.

2.4 Evaluated Configuration

The evaluated configuration consists of the following:

- a single Datacryptor SONET/SDH operating in encryption mode[3] and managed by a single instance of Element Manger running on a workstation connected via the Ethernet port.

[3] Each Datacryptor can operate in three modes: Encrypt (traffic flow between two units is encrypted), Plain (traffic flow between two units is not encrypted), and Standby (no traffic flow is transmitted).

- a single Datacryptor Gigabit Ethernet operating in encryption mode[4] and managed by a single instance of Element Manger running on a workstation connected via the Ethernet port.

The evaluation configuration also stipulates one administrator with full access privileges. Since the TOE is a point-to-point encryption device, two instances of the TOE are required to support the TOE's primary security function of encrypting traffic over an untrusted network. In order to comply with the evaluated configuration, the following hardware and software components should be used:

Table 2 - TOE Components and Version Numbers for Evaluated Configuration

TOE Component	Version/Model Number
Datacryptor SONET/SDH Hardware and Element Manager	Datacryptor SONET/SDH System Version: 4.0[5]
Datacryptor Gigabit Ethernet Hardware and Element Manager	Datacryptor Gigabit Ethernet System Version: 4.0[6]
Element Manager Host Platform	Microsoft Windows XP Service Pack 2

Note that the platform/workstation running Element Manager must be a dedicated machine; no other unnecessary third-party applications can be run. In order to maintain evaluated configuration, ports on the dedicated workstation running Element Manager that are unnecessary to the operation of the TOE (e.g., FTP, Telnet) should be disabled.

The following features are outside the scope of the TSF and thus are not evaluated:

- The ability to upgrade software/firmware components of the Datacryptor and Element Manager
- The use of SNMP for viewing of basic status and configuration details; SNMP must be disabled in the evaluated configuration.
- MAC address filtering
- Enhanced password security (Legacy password security in enabled by default, which requires passwords to be a minimum of 8 characters and a maximum of 20)
- The CLI is used for basic system provisioning and does not have access to security-relevant data; therefore, the CLI is not to be used after the TOE is configured per Administration Guidance

[4] Each Datacryptor can operate in three modes: Encrypt (traffic flow between two units is encrypted), Plain (traffic flow between two units is not encrypted), and Standby (no traffic flow is transmitted).

[5] The Datacryptor software and Element Manager software are built into the same code base when the code is compiled. As such, the Element Manager and Datacryptor share the same version number.

[6] The Datacryptor software and Element Manager software are built into the same code base when the code is compiled. As such, the Element Manager and Datacryptor share the same version number.

- The Certificate Manager is used in the initial provisioning of a Datacryptor and is not used again once the TOE is configured for evaluated configuration. The Certificate Manager can be used to generate Certificate Authority data, which can be backed up to removable media, including USB “thumb-drives” or floppy disks. Certificate Manager is not connected to the Datacryptor; the Certificate Manager resides on a stand-alone PC. The Administrator would transfer the data to the Element Manager to be loaded into the unit.

For more details and instructions to configure the TOE for evaluated configuration, please see the following:

- *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales Datacryptor SONET/SDH with Element Manager*
- *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales Datacryptor Gigabit Ethernet with Element Manager*

3. Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 - Assumptions

Assumption	Description
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.NETWORK	The TOE will be installed in a network infrastructure such that it can effectively control the flow of applicable information.
A.NOEVIL	The administrator is competent and will install and configure the TOE according to the administrator guidance.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the IT environment.

Table 4 - Threats

Threat	TOE Threats
T.ASSUME_ID_PKI_VER	A user may assume the identity of another user in order to verify a PKI signature.
T.ATTACK	An attacker (whether an insider or outsider) may gain access to the TOE and compromise its security functions by altering its configuration.

Threat	TOE Threats
T.COMP_MANAGE	Data may be compromised while traversing the connection between the Datacryptor subsystem and the Element Manager subsystem.
T.MISCONFIG	A malicious user might intentionally configure TOE security policy mechanisms incorrectly.
T.NO_ACCOUNT	An administrator might perform actions for which they are not accountable.
T.NO_DETECT	An unauthorized user, process or application attempts to mount an attack against the TOE security functions and/or associated data, which succeeds without detection.
T.SEC_BYPASS_DC	The Datacryptor subsystem might be subject to malicious tampering or bypass of its security mechanisms.
T.SEC_BYPASS_EM	The Element Manager subsystem might be subject to malicious tampering or bypass of its security mechanisms.
T.UNTRUSTED_PATH	An attacker may attempt to disclose, modify or modify frame flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality of frame flows transmitted/received over an untrusted path would be compromised.

3.4 Organisational Security Policies

There are no Organisational Security Policies identified for this TOE.

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the IT environment are designated as *OE.objective*. Objectives that apply to the non-IT environment are designated with an *ON.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives:

Table 5 - Security Objectives for the TOE

Objective	Security Objective
O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events.
O.CONFIDENTIALITY	The TOE must protect the confidentiality of frame flows transmitted to/from the TOE over an untrusted network.
O.SECURE_ACCESS	The TOE shall ensure that only authorized users are granted access to the security functions, configuration and associated data.
O.SECURE_COMM	The TOE shall securely transfer data between the Datacryptor and Element Manager subsystems.
O.SECURE_KEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt frame flows between instances of the TOE. The TOE must also provide a means of secure key distribution to other subjects.
O. SELF_PROTECT_DC	The Datacryptor subsystem will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protect itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.SELF_PROTECT_EM	The Element Manager subsystem will maintain a domain for its own execution and domains for separate application processes that protect itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.SIG_VERIFY	The TSF shall use the correct user public key for signature verification.

4.2 Security Objectives for the IT Environment

The TOE's IT environment must satisfy the following objectives:

Objective	Security Objective
OE.SELF_PROTECT_EM	For the Element Manager subsystem, the IT Environment will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protects itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.

4.3 Security Objectives for the Non-IT Environment

The TOE's Non-IT environment must satisfy the following objectives:

Table 6 - Security Objectives for the Non-IT Environment

Objective	Security Objectives for the Non-IT Environment
ON.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
ON.NETWORK	The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.
ON.NOEVIL	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of italicised items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

Security Functional Requirements are summarized in the table below:

Table 7 - Security Functional Requirements Summary

Class Heading	Class_Family	Description
Security Audit	FAU_GEN.1-NIAP-0347	Audit Data Generation
	FAU_SAR.1	Audit Review
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_CKM_SYM_EXP.1	Cryptographic Key Establishment for AES symmetric keys
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_DIG_SIG_EXP.1	Signature Blob Verification
	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1-NIAP-0407	Simple Security Attributes
	FDP_UCT.1	Basic Data Exchange Confidentiality
Identification and Authentication	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication before Any Action
Security Management	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialisation
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_RVM.1	Non-bypassability of the TSP

	FPT_RVM_SFT.1(1)	Non-bypassability of the TSP for OSs
	FPT_RVM_OS.1	Non-bypassability of the TSP for OSs
	FPT_SEP.1	Domain Separation
	FPT_SEP_SFT.1	Domain Separation for OSs
	FPT_SEP_OS.1	Domain Separation for OSs
	FPT_STM.1	Time Stamps

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1-NIAP-0347 Audit Data Generation

FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

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

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

c) [*All auditable events identified in the table below*].

Auditable events and details with applicable SFRs are listed in the following table:

Table 8 - Auditable Events and Details

SFR	Auditable Event	Details
FAU_GEN.1-NIAP-0347 Audit data generation	None	Not applicable
FAU_SAR.1 Audit review	None	Not applicable
FCS_CKM.1	None	Not applicable
FCS_CKM.4 Cryptographic key destruction	Destruction of keys	Failure of the activity
FCS_CKM_SYM_EXP.1 Cryptographic Key Establishment for AES symmetric keys	Key agreement errors	Failure of the activity
FCS_COP.1 Cryptographic operation	Crypto Engine Errors	Failure in cryptographic processing
FDP_DIG_SIG_EXP.1	Signature verification errors	Failure of the activity
FDP_IFC.1 Subset information flow control	None	Not applicable
FDP_IFF.1-NIAP-0407 Simple security attributes	None	Not applicable
FDP_UCT.1 Basic data exchange confidentiality	None	Not applicable
FIA_SOS.1 Verification	Authentication failure	Rejection by the TSF of any

SFR	Auditable Event	Details
of secrets		tested secret.
FIA_UAU.2 User authentication before any action	All uses of the authentication mechanism	Success or failure of authentication attempts
FMT_MOF.1 Management of security functions behaviour	None	Administrator actions specified in Table 10 - Management of Security Functions
FMT_MTD.1 Management of TSF data	None	Administrator actions specified in Table 11 – Management of TSF Data
FMT_SMF.1 Specification of Management Functions	None	Failure of the commissioning activity.
FMT_SMR.1 Security roles	None	Not applicable
FPT_RVM.1 Non-bypassability of the TSP	None	Not applicable
FPT_RVM_SFT.1(1) Non-bypassability of the TSP	None	Not applicable
FPT_SEP.1 TSF domain separation	None	Not applicable
FPT_SEP_SFT.1 TSF domain separation	None	Not applicable
FPT_STM.1 Reliable time stamps	None	Not applicable

FAU_GEN.1.2-NIAP-0347 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the additional information identified in the table above, column 3*].

5.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*authorised administrator*] with the capability to read [*all audit information*] from the audit records.

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

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ANSI X9.42 for Diffie-Hellman for Key Establishment*] and specified cryptographic key sizes [*256-bit AES key and 512-, 1024-, 1536- or 2048-bit P values for Diffie Hellman*] that meet the following: [*FIPS 197 for AES and ANSI X9.42 for Diffie-Hellman*].

5.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*tested by CCTL*].

5.1.2.3 FCS_CKM_SYM_EXP.1 Cryptographic Key Establishment for AES symmetric keys

Rationale for explicitly stated SFR: This SFR is necessary to define the details of ANSI X9.42 key establishment.

FCS_CKM_SYM_EXP.1.1 The cryptomodule shall provide the following cryptographic key establishment using Discrete Logarithm Key Agreement that meets the following:

a) The cryptomodule shall provide the capability to act as the initiator or responder (that is, act as Party U or Party V as defined in the standard) to agree on cryptographic keys of all sizes using the **[***dhHybrid1***]** key agreement scheme where domain parameter p is a prime of **[***1024-bit P values***]** and domain parameter q is a prime of **[***160-bit Q value***]**, and that conforms with ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography.

b) The cryptomodule shall conform to the standard using a FIPS-approved Random Number generation function and a FIPS-approved Hashing function.

c) The choices and options used in conforming to the key agreement scheme(s) are as follows: **[***prerequisites - domain parameters are validated as they are received from a trusted entity, the CM, to have validated them in accordance with sec. 7.2; public keys (Yv and Tv) are validated locally be party V using trusted routines (sec. 7.4 option 3) and party U trusts that the public keys it receives have already been validated (sec. 7.4 option 4); concatenated mode is used (sec. 7.7.2)***]**.

Application Note: Domain parameter generation is only performed by the Certificate Manager and is outside the scope of the TOE.

5.1.2.4 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [*the operations described below*] in accordance with a specified cryptographic algorithm [*multiple algorithms in the modes of operation described below*] and cryptographic key sizes [*multiple key sizes described below*] that meet the following: [*multiple standards described below*].

Table 9 - Cryptographic Operations

Operation	Algorithm (mode)	Validation Method	Key Size in Bits	Standards
Encryption and Decryption	AES (CBC mode)	Tested by CCTL	256	FIPS 197
Key agreement	Diffie-Hellman (ANSI X9.42 Hybrid 1 [concatenation])	Tested by CCTL	g = 2 p = 512, 1024, 1536 or 2048	ANSI X9.42
Hashing	SHS (SHA-1)	Tested by CCTL	160 (size of digest)	FIPS 180-2
Random Number Generation	DSS	Tested by CCTL	Not Applicable	FIPS 186-2
Digital Signatures	DSS	Tested by CCTL	Modulus Size: 1024	FIPS 186-2

5.1.3 User Data Protection (FDP)

5.1.3.1 FDP_DIG_SIG_EXP.1 Signature Blob Verification

Rationale for explicitly stated SFR: This SFR is necessary to define the details of the basic CA functionality in the TOE, which is to verify certificate details at the time of installation/commissioning.

FDP_ DIG _SIG_EXP.1.1 The TSF shall invoke the cryptographic module with the following information from Certification Path Validation to verify digital signature on signed data: subject public key algorithm, subject public key, subject public key parameters.

FDP_ DIG _SIG_EXP.1.2 The TSF shall apply the following additional checks [

1. *Verify the timeline of certificate validity*
2. *Match the subject name from the Certification Path Validation with that in the signed data.*].

5.1.3.2 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*information flow control SFP*] on [

Subject: TOE Interfaces

Information: Frame flows

Operations: Encrypt / decrypt / forward / discard

].

5.1.3.3 FDP_IFF.1-NIAP-0407 Simple Security Attributes

FDP_IFF.1.1-NIAP-0407 The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [

Subject Security Attributes:

- *HOST subject interface*
- *NET subject interface*

Information Security Attributes

- *MAC address of destination*

].

FDP_IFF.1.2-NIAP-0407 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

1. *The MAC address in the frame's Type field is not the MAC address of the TOE.*

].

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules: [

1. *A frame received by the TOE on the NET interface is discarded if a secure tunnel with a peer device is not established.*
2. *A frame received by the TOE containing the TOE's MAC address in the frame's Type field are read by the TOE and not processes for forwarding.*
3. *A frame received by the TOE on the Host interface is encrypted using the Data Encryption Key and forwarded to the untrusted network.*
4. *A frame received by the TOE on the Net interface is decrypted using the Data Encryption Key and forwarded to the trusted network side.*

].

FDP_IFF.1.4-NIAP-0407 The TSF shall provide the following [*no additional SFP capabilities*].

FDP_IFF.1.5-NIAP-0407 The TSF shall explicitly authorise an information flow based upon the following rules: [*no explicit authorisation rules*].

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based upon the following rules: [*the Data Encryption Key is not available because a secure tunnel is not established*].

5.1.3.4 FDP_UCT.1 Basic Data Exchange Confidentiality

FDP_UCT.1.1 The TSF shall enforce the [*information flow control SFP*] to be able to [transmit and receive] objects in a manner protected from unauthorised disclosure.

5.1.4 Identification and Authentication (FIA)

5.1.4.1 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*a length of 8-20 case-sensitive characters*].

5.1.4.2 FIA_UAU.2 User Authentication before Any Action

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

5.1.5 Security Management (FMT)

5.1.5.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*listed in the table below* to *authorised administrator role, as shown in the table below*.]

Table 10 - Management of Security Functions

Security Function	Authorised Administrator			
	Determine	**Disable**	**Enable**	**Modify**
Cryptographic Operations	✓	✓	✓	✓
Receiving/transmitting interface	✓	✓	✓	

5.1.5.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [*information flow control SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*specified in FDP_IFF.1-NIAP-0407*] to [*authorized administrator*].

5.1.5.3 FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.5.4 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [*information flow control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

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

5.1.5.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [change_default, query, modify, delete] the [*data described in the table below*] to [*authorised administrator*].

Table 11 - Management of TSF Data

Data	Admin			
	Change Default	Query	Modify	Delete
Admin Password	✓	✓	✓	✓
Audit Data		✓		✓
DEK/KEK Lifetimes	✓	✓	✓	
Certificate Lifetime	✓	✓	✓	
CA Public Key	✓	✓	✓	
DEK/KEK	✓	✓	✓	✓
Transmission Mode	✓	✓	✓	
System Date and Time		✓		
X.509 Certificates	✓	✓	✓	✓

5.1.5.6 FMT_SMF.1 Specification of Management Functions

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

1. *Set administrator password*
2. *Configure the TOE to establish a secure tunnel to a remote peer*
3. *Modify subject attributes and generic configuration information*

].

5.1.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*authorised administrator*].

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

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.1.6.2 FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1 The ~~TSF~~ **Datacryptor Subsystem** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.3 FPT_RVM_SFT.1 Non-Bypassability of the TSP

Rationale for explicitly stated SFR: This explicitly stated SFR states the portion of FPT_RVM supplied by the Element Manager Subsystem in support of the overall FPT_RVM functionality. See FPT_RVM.1 for the remaining TOE functionality.

FPT_RVM_SFT.1.1 The Element Manager Subsystem shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.4 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The ~~TSF~~ **Datacryptor Subsystem** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **Datacryptor Subsystem** shall enforce separation between the security domains of subjects in the TSC.

5.1.6.5 FPT_SEP_SFT.1 TSF domain separation

Rationale for explicitly stated SFR: This explicitly stated SFR states the portion of FPT_SEP supplied by the Element Manager Subsystem in support of the overall FPT_SEP functionality. See FPT_SEP.1 for the remaining TOE functionality.

FPT_SEP_SFT.1.1 The Element Manager Subsystem shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_SFT.1.2 The Element Manager Subsystem shall enforce separation between the security domains of subjects in the TSC.

5.1.6.6 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps for its own use.

5.2 Security Requirements for the IT Environment

5.2.1.1 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM.1 and FPT_RVM_SFT.1(1) (levied on the TOE) for the remaining functionality.

FPT_RVM_OS.1.1 The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed

before each function within the scope of control of the host OS is allowed to proceed.

5.2.1.2 FPT_SEP_OS.1 TSF Domain Separation for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP.1 and FPT_SEP_SFT.1 (levied on the TOE) for the remaining functionality.

FPT_SEP_OS.1.1 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_OS.1.2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3. These requirements are summarised in the following table.

Table 12 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Lifecycle Support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4 Strength of Function for the TOE

This security target includes a number of probabilistic or permutational functions. Relevant security functions and security functional requirements include:

- Identification and Authentication
    - FIA_SOS.1 – Verification of Secrets
    - FIA_UAU.2 – Authentication of administrators

The SOF for these mechanism is SOF-Basic.

The following functions are cryptographic and thus are out of scope for Strength of Function in this Security Target:

- Cryptographic support
    - FCS_COP.1 – Cryptographic Operation
    - FCS_CKM.4 – Cryptographic Key Destruction
    - FCS_CKM_SYM_EXP.1 – Cryptographic Key Establishment for AES symmetric keys

5.5 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 13 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0347	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied by FAU_GEN.1-NIAP-0347
FCS_CKM.1	No other components.	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied by FCS_CKM.4. See note below for FCS_CKM.2 and Satisfied
FCS_CKM.4	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Satisfied by FCS_CKM.1. Satisfied
FCS_CKM_SYM_EXP.1	No other components.	None.	N/A
FCS_COP.1	No other components.	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1 is satisfied by using DSS to generate random numbers for required cryptographic operations. Satisfied. FCS_CKM.4 is satisfied by overwriting keys that are established

			with the Diffie-Hellman operation.
FDP_DIG_SIG_EXP.1	No other components.	None	N/A
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied by FDP_IFF.1-NIAP-0407
FDP_IFF.1-NIAP-0407	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied by FDP_IFC.1 Satisfied
FDP_UCT.1	No other components.	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1].	The TOE does not support the ability to enforce a trusted path because the TOE does not protect against modification of frame flows. FDP_IFC.1 is satisfied
FIA_SOS.1	No other components.	None	N/A
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	The TOE does not support identity-based authentication, therefore this dependency does not apply because the TOE does not support FIA_UID.1. Administrators authenticating to the Element Manager enter only a password; there is no username to associate an identity with the Administrator.
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Satisfied by FDP_IFC.1 Satisfied Satisfied
FMT_MSA.2	No other components.	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Satisfied by FDP_IFC.1 Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	N/A
FMT_SMR.1	No other components.	FIA_UID.1	The TOE does not support identity-based authentication, therefore this dependency does not apply. Administrators authenticating to the Element Manager enter only a password; there is no username to associate an identity with the Administrator.
FPT_ITT.1	No other components.	None	N/A
FPT_RVM.1	No other components.	None	N/A
FPT_RVM_SFT.1(1)	No other components.	None	N/A
FPT_RVM_OS.1	No other components.	None	N/A
FPT_SEP.1	No other components.	None	N/A
FPT_SEP_SFT.1	No other components.	None	N/A
FPT_SEP_OS.1	No other components.	None	N/A
FPT_STM.1	No other components.	None	N/A

Notes:

- The dependency for FCS_CKM.2 is satisfied by FCS_CKM_SYM_EXP.1 and by FCS_COP.1.

6. TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

6.1.1 Security Audit

Authorized administrators the ability to access and read all auditable events using the View Logs button in the Front Panel View of Element Manager. The auditable events are categorized into columns making it easy for the authorized administrator to interpret the information; the columns are Number (for the log number), Time, Date, Type (discussed below), Event, Code, User, and Occurred. The administrator can view, search, sort, save or clear the recorded logs.

The TOE provides one log that contains data of four different types of messages:

- Audit: A report of all management operations performed on this unit (using the Element Manager).
- Error: A report of any faults that have been discovered with unit hardware and keyspace.
- Key: A report of all key update and erasure attempts.
- Trace: A report of internal software conditions detected by the unit, these are not hardware errors but may help support personnel understand unusual operational conditions. They appear on the display as 'Internal Error' but, when saved to disk as a text file, the text is expanded. When seen, these should be reported to the Support department at Thales e-Security for investigation.

The View Logs window provides sorting of audit data based on time; the authorized administrator can select the order in which entries are displayed (i.e., newest first or oldest first). The Find command in the View menu allows the authorized administrator to search through the displayed logs for specified text.

The Datacryptor subsystem includes a Real-Time Clock to stamp all log messages.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1-NIAP-0347

- FAU_SAR.1
- FPT_STM.1

6.1.2 Authentication

6.1.2.1 Authentication of Administrators

The TOE supports authentication of an administrator, who manages the TOE locally or remotely via Element Manager. The administrator is required to authenticate via password before configuring TOE security functions. Authentication credentials are stored on the PC host as a*.usr file, which contains a CA public key, User Certificate, Diffie-Hellman parameters and a Diffie-Hellman Encrypted Secret Key (DH ESK).

The password must be 8-20 characters, which is then hashed via SHA-1. The act of entering a password enables the Element Manager to decrypt the DH ESK using the hashed version of the password as the key. As the format of the DH ESK is known (it has a magic number before the data) this also enables the password to be validated by checking that the format of the DH SK is correct[7] (i.e., the user has authenticated with the PC Management Application only).

The second part of the authentication process is to authenticate with the unit to be managed. This is performed in the same manner as to peer units creating a secure tunnel as the *.usr file contains certified data signed by the same CA as is present in a unit. Therefore the exchange of certified data allows a unit to verify the trustworthiness of both the unit to manage and the PC Management Application (i.e., they are validated to belong to the same peer CA group).

The hashed values of the password do not contain a random component. As such, the same password will always generate the same respective message digest value (by nature of the SHA-1 message digest function). Therefore the Authentication function is designed to satisfy the following security functional requirements:

- FCS_COP.1
- FIA_SOS.1
- FIA_UAU.2

6.1.3 Information Flow Control

The TOE provides encryption for data traversing from one trusted network to another over SONET/SDH, and each network device allows traffic to flow between authorized sources and authorised destinations. The configuration for this data encryption is specified an Information Flow Control policy by an authorized administrator using the Element Manager software.

[7] This means that the password is never actually stored in plain text; it is stored in hashed form.

Since it provides point-to-point encryption, the TOE enforces a relatively simple information flow policy. It associates subjects with TOE interfaces when it receives traffic from those subjects (i.e., subjects with an address of the LAN correspond to the HOST interface). When the TOE receives network traffic, it will associate the destination address with the proper interface and determine the traffic should be encrypted or decrypted before transmission. The TOE will then encrypt/decrypt the traffic before forwarding via the appropriate interface. The information flow rules are restrictive by default and require configuration by an administrator before the rules can be enforced.

The Datacryptor uses an encryption algorithm for two purposes – key encryption and data encryption for user and management traffic (for management traffic, an encrypted tunnel is created between the PC and the Datacryptor in the same way as an encrypted tunnel is created between peer Datacryptor units). The following sections describe the cryptographic operations of the Datacryptor in more detail.

6.1.3.1 Verification of Certificate Authorities

Each peer Datacryptor contains a user X.509v1 certificate from a common Certificate Authority, which is loaded during the installation and initial configuration process. The certificate takes the following format:

```
Certificate                    ::=    SIGNED { SEQUENCE {
        version                [0]    Version DEFAULT v1
        serialNumber           CertificateSerialNumber
        signature              AlgorithmIdentifier
        issuer                 Name
        validity               Validity
        subject                Name
        subjectPublicKeyInfo   SubjectPublicKeyInfo
        issuerUniqueIdenfier   [1] IMPLICIT UniqueIdentifier OPTIONAL,
        subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL
```

The following table contains further information on the certificate fields:

Table 14 - Certificate Field Descriptions

Field	Description
version	1 or 3
serialNumber	Unique serial number of the actual unit (MAC address)
signature	Signing algorithm OID (will always be DSA)
issuer	Name of CA that generated the signature (specified via Certificate Manager)
validity	From and to times, as input into Element Manager during commissioning process
subject	Name of unit as set by the Element Manager
subjectPublicKeyInfo	Algorithm OID values are DH and the DH public key (modulus and prime numbers)
issuerUniqueIdenfier	Not used (only implemented in X.509v2)
subjectUniqueIdentifier	Not used (only implemented in X.509v2)

The signature on the certificate is verified by the Datacryptor's data authentication implementation (DSA). By verifying and accepting the Certificate Authority signature,

the TOE will ensure that only Certificate Authorities that have been signed by an authorised body may be used to verify the signature on key exchange keysets.

6.1.3.2 Verification of Key Exchange Algorithm Keysets

During the TOE installation and configuration process, Key Exchange Algorithm Keysets signed by a CA are loaded. The signature on the keyset is verified by the Datacryptor's data authentication implementation. The keyset is accepted upon successful verification.

Instances of the TOE also exchange signed key exchange certificates during the key exchange protocol. Both instances must positively verify that the keyset has been authorised by an approved CA before proceeding to generate a shared Key Encryption Key.

6.1.3.3 Key Agreement Algorithm

A secure key exchange algorithm allows two instances of the TOE to establish a common Key Encryption Key (KEK) without either party having to transmit any secret data. An implementation of a secure key exchange algorithm is used for this purpose, which requires the input of both subject's signed public and secret keys. In addition to these values, each subject inputs a random one-time public-secret key pair using the FIPS-approved pseudo-random number generator (DSS/FIPS 186-2), ensuring that every KEK generated between the subjects is unique.

6.1.3.4 Key Encryption

After deriving a Key Encryption Key, the subjects must securely derive a Data Encryption Key (DEK) to encrypt traffic between them. To generate a DEK, entities use their KEK to encrypt random data generated by the FIPS-approved pseudo-random number generator. The result is sent to the other subject, where it is decrypted with the KEK. Each subject concatenates both sets of random data to generate a DEK.

6.1.3.5 Data Encryption and Decryption

The encryption algorithm (AES) uses the Data Encryption Key to encrypt traffic transmitted to another instance of the TOE and to decrypt traffic received from another instance of the TOE.

6.1.3.6 Key Destruction

The Data Encryption Key and the Key Encryption Key are deleted at intervals defined by the administrator via Element Manager or by forcing generation of new keys. Keys are zeroized and deleted according to specifications in FIPS 140-2.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.4
- FCS_CKM_SYM_EXP.1
- FCS_COP.1
- FDP_DIG_SIG_EXP.1

- FDP_IFC.1
- FDP_IFF.1-NIAP-0407
- FDP_UCT.1

6.1.4 Security Management

The TOE is managed via GUI interface called Element Manager, and access can be obtained remotely via the Ethernet interface. The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfil the security objectives if the TOE. Security Management principles relate to Security Audit, Information Flow Control, and Cryptographic Support.

The TOE maintains one role, and this role has full administrator privileges including configuration of information flow control policies and overall TOE configuration. Privileges are defined by access to the *.usr file and associated password, and the Administrator has the following privileges:

- read/write access to unit communications properties
- read/write access to unit security properties
- read/write access to unit logs

This information is also exchanged during the establishment of secure tunnel to the Datacryptor, so that the Datacryptor can also enforce the available commands that an administrator may perform.

The TOE allows the administrator to manage its policies, and the TOE enforces no information flow policies by default. Only an administrator can change the initial default settings/security attributes.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1
- FMT_MSA.1
- FMT_MSA.2
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

6.1.5 Protection of Security Functions

The TOE provides various protection mechanisms for its security functions, including requiring the administrator to authenticate before any administrative operations can be performed on the system. The Datacryptor subsystem is self-contained; therefore, it maintains its own execution domain and the device performs all intrinsic security functions.

The Element Manager subsystem and its environment protects security functions via the host OS, which maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

Communications between each subsystem (Datacryptor and Element Manager) is protected via encrypted tunnel. This tunnel is derived in exactly the same way as a tunnel between instances of the TOE (e.g., tunnels for the HOST and NET interfaces). When a terminal running Element Manger is connected to the RS-232 port, communications are protected via physical connection to the Datacryptor unit itself.

The Protection of Security Functions function is designed to satisfy the following security functional requirements:

- FPT_ITT.1
- FPT_RVM.1
- FPT_RVM_SFT.1(1)
- FPT_RVM_OS.1
- FPT_SEP.1
- FPT_SEP_SFT.1
- FPT_SEP_OS.1

7. Protection Profile Claims

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

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functions.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 15 - Threats and Assumptions to Security Objectives Mapping

Threat / Assumption \ Objective	O.AUDIT_GEN	O.CONFIDENTIALITY	O.SECURE_ACCESS	O.SECURE_COMM	O.SECURE_KEY	O.SELF_PROTECT_DC	O.SELF_PROTECT_EM	O.SIG_VERIFY	OE.SELF_PROTECT_EM	ON.ENVIRON	ON.NETWORK	ON.NOEVIL
T.ASSUME_ID_PKI_VER								✓				
T.ATTACK			✓									
T.COMP_MANAGE				✓								
T.MISCONFIG			✓									✓
T.NO_ACCOUNT	✓											
T.NO_DETECT	✓											
T.SEC_BYPASS_DC						✓						
T.SEC_BYPASS_EM							✓		✓			
T.UNTRUSTED_PATH		✓			✓							
A.ENVIRON										✓		
A.NETWORK											✓	
A.NOEVIL												✓

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 16 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ASSUME_ID_PKI_VER A user may assume the identity of another user in order to verify a PKI signature.	**O.SIG_VERIFY** mitigates this threat by ensuring that the TSF uses the correct public keys for signature verification.
T.ATTACK An attacker (whether an insider or outsider) may gain access to the TOE and compromise its security functions by altering its configuration.	**O.SECURE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication, mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user.
T.COMP_MANAGE Data may be compromised while traversing the connection between the Datacryptor subsystem and the Element Manager subsystem.	**O.SECURE_COMM** mitigates this threat ensuring that data is transferred securely between physically separate components (i.e., when configuring the Datacryptor via Element Manager over the Ethernet interface).
T.MISCONFIG A malicious user might intentionally configure TOE security policy mechanisms incorrectly.	**O.SECURE_ACCESS** helps to mitigate this threat by ensuing that only authorized users (i.e., administrators) an configure the TOE security functions. **ON.NOEVIL** helps to mitigate this threat by ensuring that administrators will adhere to applicable guidance when installing and configuring the TOE security functions
T.NO_ACCOUNT An administrator might perform actions for which they are not accountable.	**O.AUDIT_GEN** mitigates this threat by recording actions for later review
T.NO_DETECT An unauthorized user, process or application attempts to mount an attack against the TOE security functions and/or associated data, which succeeds without detection.	**O.AUDIT_GEN** helps to mitigate this threat by providing the Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events.
T.SEC_BYPASS_DC The Datacryptor subsystem might be subject to malicious tampering or bypass of its security mechanisms.	**O.SELF_PROTECT_DC** contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat.

T.TYPE	Security Objectives Rationale
T.SEC_BYPASS_EM The Element Manager subsystem might be subject to malicious tampering or bypass of its security mechanisms.	**O.SELF_PROTECT_EM** contributes to countering this threat by ensuring that the Element Manager portion of the TSF can protect itself from users within the TSC. If this TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. **OE.SELF_PROTECT_EM** contributes to countering this threat by ensuring that the OS can protect itself from users within its control. If the OS could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the executable code of the Element Manager subsystem.
T.UNTRUSTED_PATH An attacker may attempt to disclose, modify or modify frame flows transmitted/received by the TOE over an untrusted network. If such an attack was successful, then the confidentiality of frame flows transmitted/received over an untrusted path would be compromised.	**O.CONFIDENTIALITY** mitigates this threat by ensuring that the confidentiality of data flows is maintained during transmission. **O.SECURE_KEY** mitigates this threat by ensuring that cryptographic keys are kept confidential.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 17 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.	**ON.ENVIRON** addresses this assumption by requiring the Administrator to install the TOE in a physically secure environment with adequate infrastructure to provide reliable operation.
A.NETWORK The TOE will be installed in a network infrastructure such that it can	**ON.NETWORK** addresses this assumption by ensuring that that the platforms used to host the TOE conform to the hardware, software, and installation outlined in the administrator guidance. The administrator will reference this guidance while provisioning and maintaining the TOE, and the guidance contains specific instructions for installation into the network infrastructure.

A.TYPE	Environment Security Objective Rationale
effectively control the flow of applicable information.	
A.NOEVIL The administrator is competent and will install and configure the TOE according to the administrator guidance.	**ON.NOEVIL** addresses this assumption by ensuring that administrators will adhere to applicable guidance when installing and configuring the TOE security functions

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 18 - SFRs to Security Objectives Mapping

Objective / SFR	O.AUDIT_GEN	O.CONFIDENTIALITY	O.SECURE_ACCESS	O.SECURE_COMM	O.SECURE_KEY	O.SELF_PROTECT_DC	O.SELF_PROTECT_EM	O.SIG_VERIFY	OE.SELF_PROTECT_EM
FAU_GEN.1-NIAP-0347	✓								
FAU_SAR.1	✓								
FCS_CKM.1					✓				
FCS_CKM.4					✓				
FCS_CKM_SYM_EXP.1					✓				
FCS_COP.1		✓		✓	✓				
FDP_DIG_SIG_EXP.1								✓	
FDP_IFC.1		✓							

Objective / SFR	O.AUDIT_GEN	O.CONFIDENTIALITY	O.SECURE_ACCESS	O.SECURE_COMM	O.SECURE_KEY	O.SELF_PROTECT_DC	O.SELF_PROTECT_EM	O.SIG_VERIFY	OE.SELF_PROTECT_EM
FDP_IFF.1-NIAP-0407		✓							
FDP_UCT.1		✓							
FIA_SOS.1			✓						
FIA_UAU.2			✓						
FMT_MOF.1			✓						
FMT_MSA.1			✓						
FMT_MSA.2			✓						
FMT_MSA.3			✓						
FMT_MTD.1			✓						
FMT_SMF.1			✓						
FMT_SMR.1			✓						
FPT_ITT.1				✓					
FPT_RVM.1					✓	✓			
FPT_RVM_SFT.1(1)					✓		✓		
FPT_RVM_OS.1									✓
FPT_SEP.1					✓	✓			
FPT_SEP_SFT.1					✓		✓		
FPT_SEP_OS.1									✓
FPT_STM.1	✓								

The following table provides the detail of TOE security objective(s).

Table 19 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT_GEN The TOE will provide the capability to detect and create records of security-relevant events.	**FAU_GEN.1-NIAP-0347** defines the set of events that the TOE must be capable of recording. This requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. **FAU_SAR.1** provides the Administrator with the capability to read the audit data contained in the audit trail. The Administrator can examine

Security Objective	SFR and Rationale
	(via Element Manager) an audit record and have the appropriate information presented together to facilitate the analysis of the audit review. **FPT_STM.1** provides reliable time stamps for audit data.
O.CONFIDENTIALITY The TOE must protect the confidentiality of frame flows transmitted to/from the TOE over an untrusted network.	**FCS_COP.1** ensures that the establishment of the trust relationship and the confidentiality operations are cryptographically sound. All frame flows and Element Manager data are encrypted with 256-bit AES. **FDP_IFC.1** identifies and defines the information flow control SFP and the scope of control of the policies that form the identified information flow control portion of the TSP**.** **FDP_IFF.1-NIAP-0407** states the rules for traffic exchange with a peer. Frames received on the HOST interface are encrypted with the DEK and forwarded to a peer via the NET interface. Frames received on the NET interface are decrypted with the DEK and forwarded to a peer via the HOST interface. **FDP_UCT.1** provides confidentiality for frame flows received by, or transmitted from, the TOE using key material associated with an identified remote IT system.
O.SECURE_ACCESS The TOE shall ensure that only authorized users are granted access to the security functions, configuration and associated data.	**FIA_SOS.1** defines the minimum password requirements for the TOE. **FIA_UAU.2** requires that a user be authenticated by the TOE before allowing any actions on behalf of that user. **FMT_MOF.1** requires that the ability to use particular TOE capabilities be restricted to the Administrator. **FMT_MSA.1** specifies the rules for managing security attributes used in information flow control decisions, which can only be accessed by an authorized administrator **FMT_MSA.2** requires that only secure values be accepted by the TOE for security attributes. **FMT_MSA.3** requires the TOE to impose restrictive default values for security attributes in all cases. **FMT_MTD.1** requires that the ability to manipulate TOE content is restricted to Administrators. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported.
O.SECURE_COMM The TOE shall securely transfer data between the Datacryptor and Element Manager subsystems.	**FCS_COP.1** requires encryption of data between the Element Manger and the Datacryptor for remote administration. **FPT.ITT.1** requires that the TOE protects TSF data from one component to another.

Security Objective	SFR and Rationale
O.SECURE_KEY The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt frame flows between instances of the TOE. The TOE must also provide a means of secure key distribution to other subjects.	**FCS_CKM.1** ensures that the KEK, DEK, and DH P value are generated with standards-based algorithms. **FCS_CKM.4** ensures that the KEK and DEK keys are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications. **FCS_COP.1** ensures that the establishment of the trust relationship and the key exchange operations are cryptographically sound. **FPT_RVM.1** ensures that the TOE enforcement functions for the Datacryptor Subsystem are successful before allowing access to keys. **FPT_RVM_SFT(1)** ensures that the TOE enforcement functions for the Element Manager Subsystem are successful before allowing access to keys **FPT_SEP.1** ensures that the Datacryptor Subsystem TSF is protected against interference and tampering by untrusted subjects. **FPT_SEP_SFT.1** ensures that the Element Manager subsystem TSF is protected against interference and tampering by untrusted subjects.
O. SELF_PROTECT_DC The Datacryptor subsystem will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protects itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.	**FPT_RVM.1** ensures that the Datacryptor subsystem always enforces its information flow control and authentication rules at the applicable interfaces. **FPT_SEP.1** ensures that the TSF is protected against interference and tampering by untrusted subjects.
O.SELF_PROTECT_EM The Element Manager subsystem will maintain a domain for its own execution and domains for separate application processes that protect itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.	**FPT_RVM_SFT.1(1)** ensures that the Element Manager subsystem TSF always enforces its information flow control and authentication rules at the applicable interfaces. **FPT_SEP_SFT.1** ensures that the Element Manager subsystem TSF is protected against interference and tampering by untrusted subjects.
O.SIG_VERIFY The TSF shall use the correct user public key for signature verification.	**FDP_DIG_SIG_EXP.1** ensures that the TOE uses standards-based signature verification techniques.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

The following table provides the detail of IT Environment security objective(s):

Table 20 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
OE.SELF_PROTECT_EM For the Element Manager subsystem, the IT Environment will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protects itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.	**FPT_SEP_OS.1** ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment. **FPT_RVM_OS.1** ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are within the TSC. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL3. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 21 - Assurance Measures

Component ID	Rationale
ACM_CAP.3	Authorisation controls: The implementation and documentation of procedures for controls to ensure that unauthorised modifications are not made to the TOE and to ensure proper use/functionality of the CM system. Evidence Titles: • *Configuration Management Plan: Thales e-Security Datacryptor SONET/SDH with Element Manager* • *Configuration Management Plan: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
ACM_SCP.1	TOE CM coverage: Documentation specifying the placement of the TOE implementation and evaluation evidence under CM. Evidence Titles: • *Configuration Management Plan: Thales e-Security Datacryptor SONET/SDH with Element Manager*

Component ID	Rationale
	• *Configuration Management Plan: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
ADO_DEL.1	Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner. Evidence Titles: • *Secure Delivery Processes and Procedures: Thales e-Security Datacryptor SONET/SDH with Element Manager* • *Secure Delivery Processes and Procedures: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
ADO_IGS.1	Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner. Evidence Titles: • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor SONET/SDH with Element Manager* • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
ADV_FSP.1	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Titles: • *Functional Specification: Thales Datacryptor SONET/SDH with Element Manager* • *Functional Specification: Thales Datacryptor Gigabit Ethernet with Element Manager*
ADV_HLD.2	Security enforcing high-level design: System Design for the TOE providing descriptions of the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate. Evidence Titles: • *High Level Design and Correspondence Analysis: Thales Datacryptor SONET/SDH with Element Manager* • *High Level Design and Correspondence Analysis: Thales Datacryptor Gigabit Ethernet with Element Manager*
ADV_RCR.1	Informal correspondence demonstration: The documentation of the correspondence between the TSS, FSP and HLD in specifically provided deliverables. Evidence Titles: • *High Level Design and Correspondence Analysis: Thales Datacryptor SONET/SDH with Element Manager* • *High Level Design and Correspondence Analysis: Thales Datacryptor Gigabit Ethernet with Element Manager*
AGD_ADM.1	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Titles: • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor SONET/SDH with Element*

Component ID	Rationale
	Manager • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
AGD_USR.1	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Titles: • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor SONET/SDH with Element Manager* • *Administrative Guidance and Installation, Generation, and Startup Procedures: Thales e-Security Datacryptor Gigabit Ethernet with Element Manager*
ALC_DVS.1	Identification of security measures: The documentation of development security documentation that describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Evidence Titles: • *Identification of Security Measures: Thales Datacryptor SONET/SDH with Element Manager* • *Identification of Security Measures: Thales Datacryptor Gigabit Ethernet with Element Manager*
ATE_COV.2	Evidence of coverage: Documented systematic testing of the TSF against the functional specification. Evidence Title: *Test Coverage Analysis: Thales e-Security Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager*
ATE_DPT.1	Testing: high-level design: Documents testing at the subsystem level to demonstrate the presence of any flaws. The tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. Evidence Title: *Datacryptor SONET/SDH & Datacryptor GigE Common Software Release 4.0 System Test Procedure*
ATE_FUN.1	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *Datacryptor SONET/SDH & Datacryptor GigE Common Software Release 4.0 System Test Procedure*
ATE_IND.2	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: N/A
AVA_MSU.1	Examination of guidance: Documentation that ensures that the guidance documentation does not contain misleading or conflicting guidance. Evidence Title: N/A
AVA_SOF.1	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment.

Component ID	Rationale
	Evidence Title: *Strength of Function Analysis: Thales Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager*
AVA_VLA.1	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are countered. Evidence Title: *Vulnerability Assessment: Thales Datacryptor SONET/SDH with Element Manager and Gigabit Ethernet with Element Manager*

8.2.3.2 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs. The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 22 - SFRs to TOE Security Functions Mapping

TSF / SFR	AUTHENTICATION	SECURITY AUDIT	INFORMATION FLOW CONTROL	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS
FAU_GEN.1-NIAP-0347		✓			
FAU_SAR.1		✓			
FCS_CKM.1			✓		
FCS_CKM.4			✓		
FCS_CKM_SYM_EXP.1			✓		

TSF / SFR	AUTHENTICATION	SECURITY AUDIT	INFORMATION FLOW CONTROL	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS
FCS_COP.1	✓		✓		
FDP_DIG_SIG _EXP.1			✓		
FDP_IFC.1			✓		
FDP_IFF.1-NIAP-0407			✓		
FDP_UCT.1			✓		
FIA_SOS.1	✓				
FIA_UAU.2	✓				
FMT_MOF.1				✓	
FMT_MSA.1				✓	
FMT_MSA.2				✓	
FMT_MSA.3				✓	
FMT_MTD.1				✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	
FPT_ITT.1					✓
FPT_RVM.1					✓
FPT_RVM_SFT.1(1)					✓
FPT_RVM_OS.1					✓
FPT_SEP.1					✓
FPT_SEP_SFT.1					✓
FPT_SEP_OS.1					✓
FPT_STM.1		✓			

Table 23 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1-NIAP-0347	The Security Audit function supports this SFR by ensuring that the TOE generates audit logs from the audit of a variety of security events.
FAU_SAR.1	The Security Audit function supports this SFR by enabling only authorized users to review and query the audit logs based on the certain criteria.
FCS_CKM.1	The Information Flow Control function supports this SFR by ensuring that the TOE supports strong, standards-based methods for cryptographic key generation.
FCS_CKM.4	The Information Flow Control function supports this SFR by providing secure, standards-based key destruction as specified in FIPS 140-2.
FCS_CKM_SYM_EXP.1	The Information Flow Control function supports this SFR by providing secure, standards-based key distribution as specified in ANSI X9.42.
FCS_COP.1	The Information Flow Control function supports this SFR by ensuring that the TOE supports strong, standards-based cryptographic methods for the following cryptographic operations: data encryption and decryption, digital signature generation and verification, cryptographic key encryption and decryption, and cryptographic key agreement. The Authentication function supports this SFR by ensuring that administrator passwords are hashed with SHA-1 and compared to the stored hash value. A value match results in successful authentication.
FDP_DIG_SIG_EXP.1	The Information Flow Control function supports this SFR by utilizing an on-board CA to verify certificate details during the installation/commissioning process.
FDP_IFC.1	The Information Flow Control function supports this SFR by utilizing the information process flow policy to monitor and process the data entering the Datacryptor subsystem.
FDP_IFF.1-NIAP-0407	The Information Flow Control function supports this SFR by enforcing the configured security policy rules for information flow.
FDP_UCT.1	The Information Flow Control function supports this SFR by providing confidentiality for data received and transmitted by the TOE using key material agreed with another TOE
FIA_SOS.1	The Authentication security function supports this SFR by providing a mechanism to verify that secrets meet a minimum level of security.
FIA_UAU.2	The Authentication security function supports this SFR by requiring each user to successfully authenticate using a unique password prior to performing any action on the TOE.
FMT_MOF.1	The Security Management security function supports this SFR by restricting the ability to manage information flow security function to an authorized administrator.
FMT_MSA.1	The Security Management security function supports this SFR by specifying that only an authorized administrator can manage security attributes used in information flow control decisions.
FMT_MSA.2	The Security Management security function supports this SFR by ensuring that that only secure values be accepted by the TOE for security attributes.

SFR	SF and Rationale
FMT_MSA.3	The Security Management security function supports this SFR by requiring only authorized administrators to specify alternative values to override the restrictive default values for security attributes.
FMT_MTD.1	The Security Management security function supports this SFR by restricting the ability to configure the TOE to uphold the information flow control policies.
FMT_SMF.1	The Security Management security function supports this SFR by providing the TOE Administrator the capability to enable and disable the information process flow policy, select the actions that would be taken upon the violation of the policy and select the method and type of notification of violations. It provides the capability for the administrator the ability to install and configure the TOE services to ensure that the information entering the system is subjected to the information process flow policy.
FMT_SMR.1	The Security Management security function supports this SFR by assigning each user to the role of Administrator.
FPT_ITT.1	The Protection of Security Functions function supports this SFR by protecting TSF data from when it is transmitted between separate parts of the TOE
FPT_RVM.1	The Protection of Security Functions function supports this SFR by ensuring that all information traffic is subjected to the information process flow policy.
FPT_RVM_SFT.1(1) and FPT_RVM_OS.1	The Protection of Security Functions function supports this SFR by ensuring that all information traffic is subjected to the information process flow policy.
FPT_SEP.1	The Protection of Security Functions function supports this SFR by providing protection mechanisms for its security functions, such as the restricted ability that only TOE Administrators can perform administrative actions on the TOE.
FPT_SEP_SFT.1 and FPT_SEP_OS.1	The Protection of Security Functions function supports this SFR by providing protection mechanisms for its security functions, such as the restricted ability that only TOE Administrators can perform administrative actions on the TOE.
FPT_STM.1	The Security Audit function supports this SFR by utilising the internal time source security function (i.e., a real time clock) implemented by the Datacryptor subsystem. It is used to ensure that each audited event contains a date and time stamp for that event.

8.4 PP Claims Rationale

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

8.5 Strength of Function Rationale

This security target includes a number of probabilistic or permutational functions of a non-cryptographic nature. Relevant security functions and security functional requirements include:

- Identification and Authentication
    - FIA_SOS.1 – Verification of Secrets
    - FIA_UAU.2 – Authentication of administrators

Part 1 of the CC defines "Strength of Function (SOF)" in terms of the minimum efforts assumed necessary to defeat the expected security behaviour of a TOE security function. There are three Strength of Function levels defined in Part 1:

- SOF-basic
- SOF-medium
- SOF-high.

The claimed minimum strength of function for this Security Target is SOF-basic, which is defined in CC Part 1 section 2.3 as:

> A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST. The attributes chosen for inclusion in this ST were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.