Security Target

Nokia
1830 Photonic Service Switch (PSS)

Table of Contents

List of Tables

List of Figures

1. Security Target Introduction

This Security Target is for the Common Criteria evaluation of the Nokia 1830 Photonic Service Switch (PSS) for DWDM (Dense Wavelength Division Multiplexing) networks based on Nokia's 1830 Photonic Service Switch (PSS) and the 11QPEN4 (Quad Port 10G Encryption) and S13X100E (Single Port 100G Encryption) Transponders.

The 1830 PSS is a scalable DWDM platform that supports aggregation for Ethernet, Fibre Channel (FC) and other protocols. DWDM is an optical multiplexing technology used to increase bandwidth in the same fiber by combining and transmitting multiple signals simultaneously over different wavelengths. The 11QPEN4 and S13X100E are pluggable cards for 1830 PSS platform providing Layer 1 data encryption.

Layer 1 encryption provides end-to-end protection against loss of confidentiality along the fiber. Encryption at this layer also allows independence in the selection of protocols or applications used at higher layers, as well as lower encryption latency.
The 11QPEN4 is a 10G, Quad port, any-rate module with four optical fiber interfaces. This module supports four independent multi-rate 10G channels and is provided in a kit which includes the card and software license for encryption for one port. A 10G pluggable line port of the 11QPEN4 supports 88 channels when configured with a tunable XFP. The module provides AES-256-CTR (Counter) encryption or AES-256-GCM (Galois Counter Mode) encryption/authentication for up to four separate 8G/10G signals and adds this functionality in the same footprint used for optical transponder functions without reducing shelf or the system capacity.
The S13X100E is a 100G single line port module, which supports 10G, 40G and 100G client signals. The line side optics of the S13X100E can support a tuning range of 9130.000 ... 9605.000 in steps of 6.25GHz (DWDM flexgrid frequencies). The module provides AES-256-CTR (Counter) encryption with AES-256-GMAC (Galois Message Authentication Code) authentication at the 100G line port.

For the complex security scenarios such as government organizations, healthcare and financial institutions, the Nokia 1830 PSS also allows secure interworking with off-the-shelf key management systems that cover the lifecycle of cryptographic services in the datacenter, namely the key generation, distribution, activation, rotation and destruction.

1.1 Security Target Identification

Name:	Security Target Nokia 1830 Photonic Service Switch (PSS) R13.1.4
Version:	1.1
Publication Date:	31 March 2026
Author:	Nokia Optical Division

1.2 TOE Identification

Name:	1830 Photonic Service Switch (PSS)
Version:	R13.1.4 (Comprises SW identification of R13.1-4)
Sponsor:	Nokia
Developer:	Nokia
Keywords:	DWDM, datacenter, interconnection, encryption

The evaluation is performed on three 1830 PSS configurations (PSS-32 / PSS-16II / PSS-8) (see section 1.5.1.2).

The key management tool (KMT) is the SMS (Security Management Server), which is part of the TOE. The SMS Security Target is defined in a separate document.

1.3 Abbreviations, Terminology and References

1.3.1 Abbreviations

The following abbreviations are used in this document.

Term	Description
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CC	Common Criteria
CIT	Craft Interface Terminal
CMVP	Cryptographic Module Validation Program
CTR	Counter Mode
DoS	Denial of Service
DWDM	Dense Wave Division Multiplexing
EAL	Evaluation Assurance Level
EC	Equipment Controller
EMS	Equipment Management System
FC	Fiber Channel
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GCM	Galois Counter Mode
GE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
IPsec	Internet Protocol security
KGF	Key Generation Functionality
KMF	Key Management Functionality
KMT	Key Management Tool
MIB	Management Information Base (the management model used for SNMP)
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
OSP	Organizational Security Policy
OTU	Optical Transport Unit
PSS	Photonic Service Switch
QPEN	Quad Port Encryption Transponder
RBAC	Role Based Access Control
SAM	Service Aware Manager
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHS	Secure Hash Standard
SLA	Service Level Agreement

Term	Description
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Secure Network Management Protocol
TL1	A Management Interface based on Transaction Language 1
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
uBCM	Micro Board Control Module
VOA	Variable Optical Attenuator
WKAT	Well-Known Answer Test
XFP	10 Gigabit Small Form Factor Pluggable

Table 1.1: Abbreviations

1.3.2 Terminology

Terms defined in the [CC] are not reiterated here, unless stated otherwise.

1.3.3 References

Abbreviation	Document
[CC]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017, CCMB-2017-04-(001 to 003)
[CCP1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
[CCP2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
[CCP3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
[cPP_ND]	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14-March-2018
[FIPS]	FIPS PUB 140-2. Security Requirements for Cryptographic Modules. May 2001
[ITU_1]	ITU-T Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications, March 1991
[ITU_2]	ITU-T Recommendation X.805: Security Architecture for Systems Providing End-to-End Communications, October 2003
[SP800-38D]	NIST Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[GdMC]	ANSSI Recommendation on selection and use of cryptographic algorithms: Guide des mécanismes cryptographiques Contained documents: Guide de sélection d'algorithmes cryptographiques v1.0, March 2021 Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques v2.04, January 2020

Table 1.2: References

1.4 Target of Evaluation (TOE) Overview

Nokia 1830 Photonic Service Switch (PSS) is based on the encryption cards 11QPEN4 and S13X100E installed on an 1830 PSS shelf with an Equipment Controller (EC). The TOE consists of both hardware and software as shown in Figure 1, Figure 2, Figure 3 and Figure 4 and identified in shaded areas.

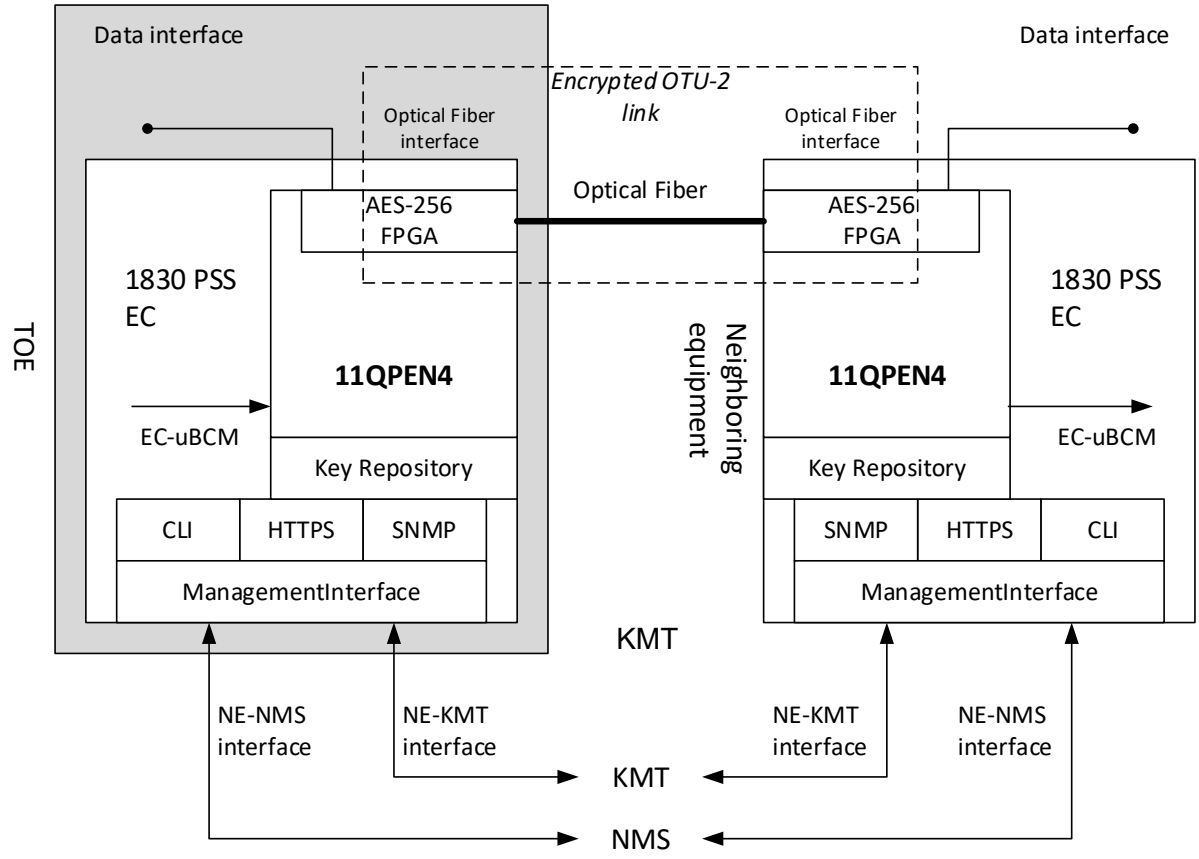


Figure 1 – 1830 Photonic Service Switch (PSS) with 11QPEN4

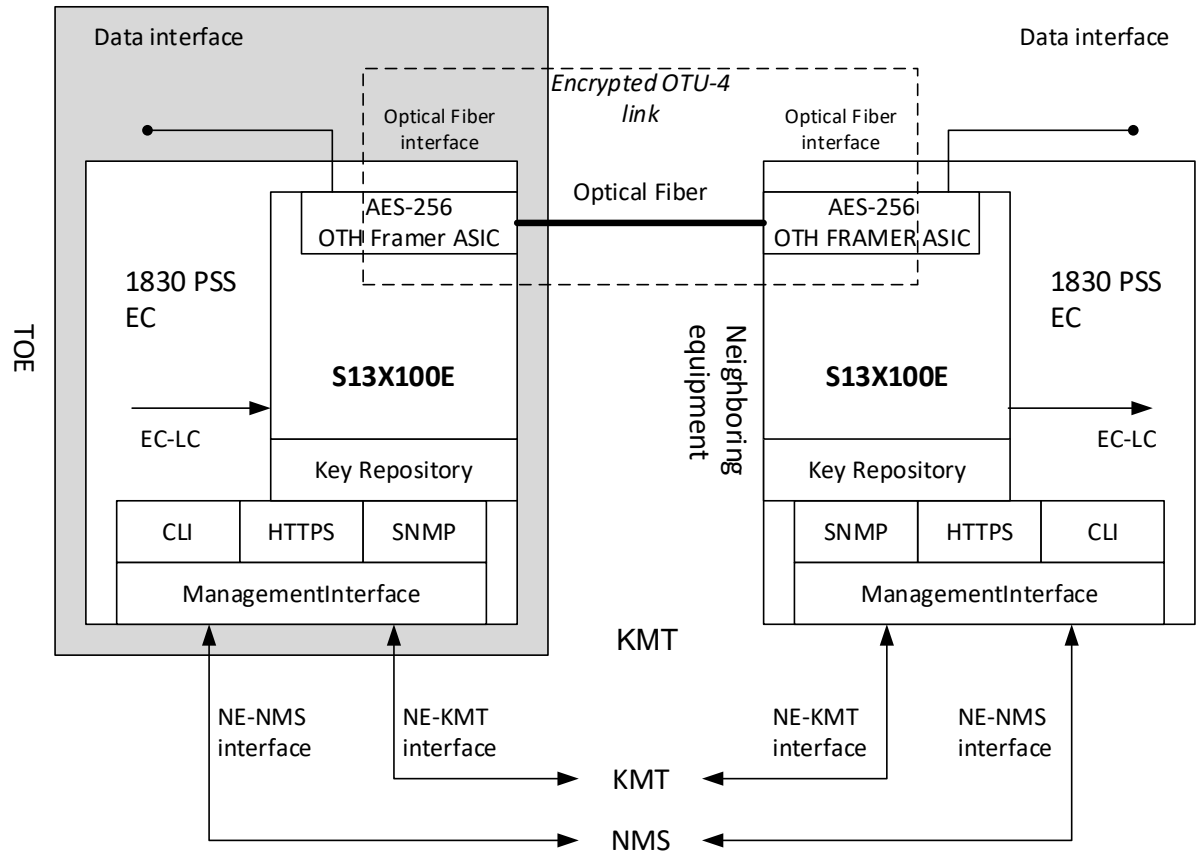


Figure 2 – 1830 Photonic Service Switch (PSS) with S13X100E

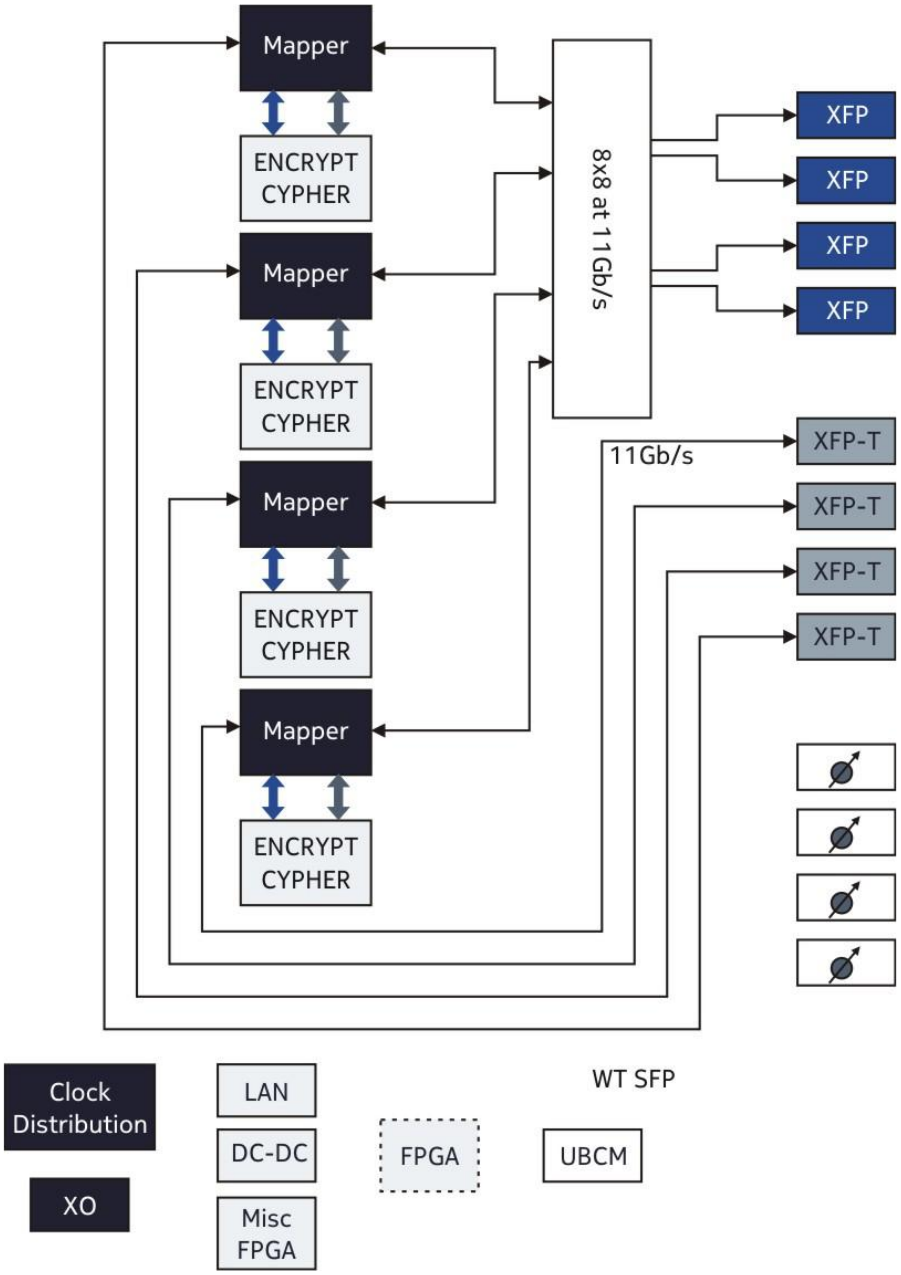


Figure 3 – 1830 Photonic Service Switch (PSS) - 11QPEN4 schematics

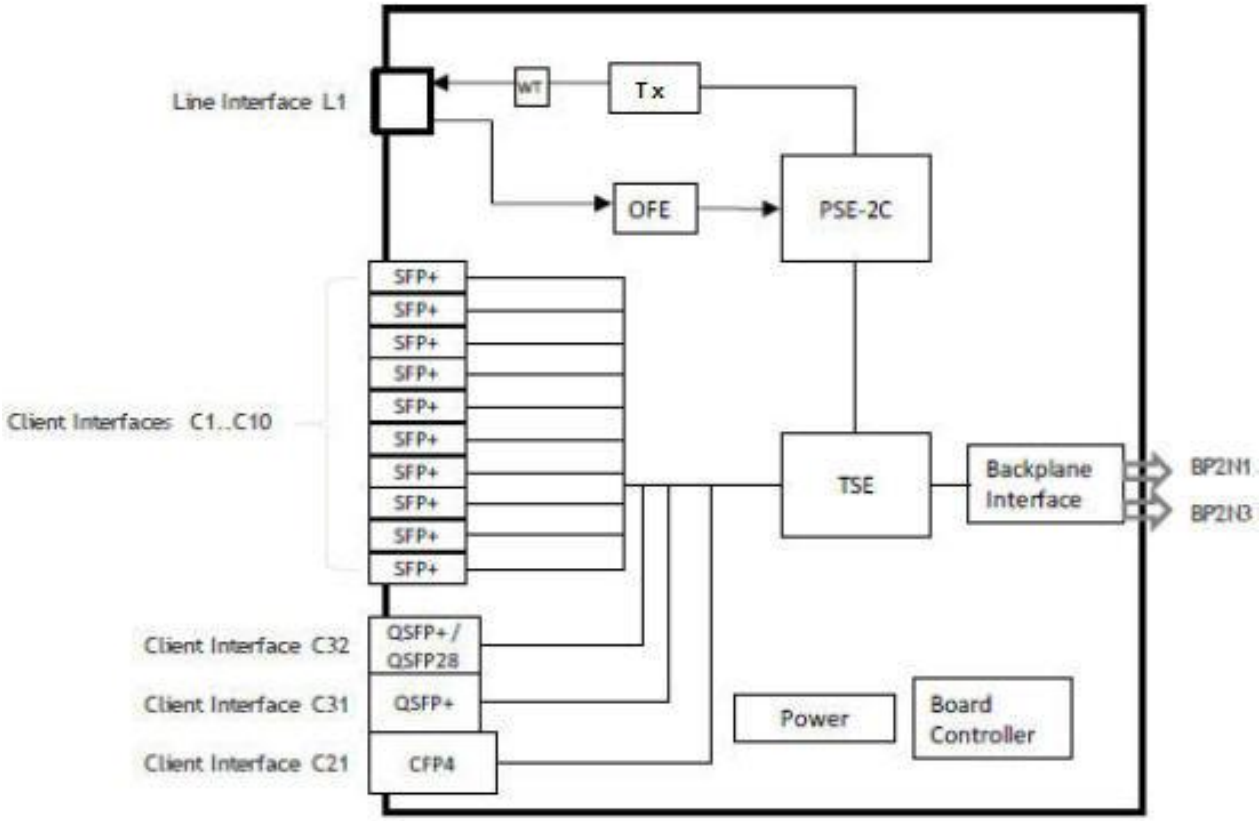


Figure 4 – 1830 Photonic Service Switch (PSS) – S13X100E schematics

The interfaces covered by the TOE are:

a) The data interfaces to connect external client equipment;

b) The Optical Fiber interfaces to connect the TOE to similar neighboring equipment; and

c) The Management Interface to configure and manage the TOE.

The S13X100E R13.1.4-ECE software does not support configuration nor use of Backplane Interface [BP2N1, BP2N3] on the S13X100E.

The security features covered by the TOE are:

a) Cryptographic Support;

b) Secure Management;

c) Self-testing;

d) User Authentication, Authorization and Audit Logs; and

e) Potential Intrusion Alarms.

For this evaluation, the only allowed KMT is the SMS (Security Management Server).

1.5 TOE Description

1.5.1 System Overview

The TOE is integrated into a subsystem composed of Neighboring Equipement (NE) and a management system. The following drawing gives a general overview of the system architecture and interconnections.

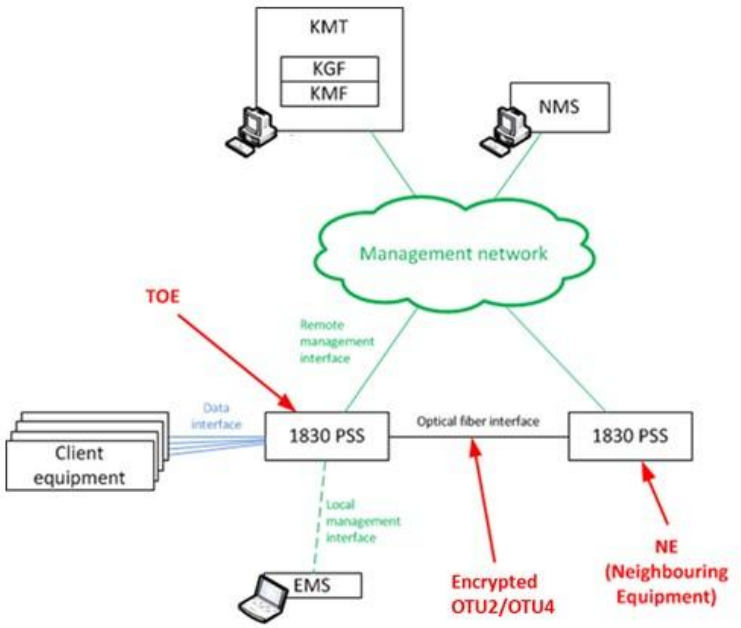


Figure 5 – System overview

The TOE (1830 PSS) is connected to a remote NE through an optical fiber link. They communicate using the OTU-2 (11QPEN4) or OTU-4 (S13X100E) protocol, with an encrypted payload.
The KMT (Key Management Tool), composed of a KGF (Key Generation Functionality) and a KMF (Key Management Functionality), generates and distributes traffic session keys used by the TOE and its NEs to encrypt the payload of OTU-2 or OTU-4 communications. The KMT is based on a Bull/ATOS HSM (Hardware Security Module) Proteccio appliance.
The NMS (Network Management System) offers a remote network management capabilities (provioning of links between 1830 PSS, …) and users management.
The EMS (Equipment Management System) allows to perform initial configuration and provisioning of the TOE and other local management activities.

The typical operational environment of the TOE may consist of the following external hardware and software in the customer's Operational Environment.

Environment	Purpose	Applicable Standards
Neighboring Equipment	As Neighboring Equipment, it is defined as a second 1830 PSS connected via the optical fiber to the TOE in a remote site as shown in Figure 1 or Figure 2.	ITU-T G.709 and Advanced Encryption Standard AES-256 in CTR mode, [SP800-38D] for GCM and GMAC
Equipment Management System (EMS)	The EMS is an external system or equipment that can be used to administer and operate the TOE via the Local Management Interface. EMS communicates with the TOE through CLI over Serial port, CLI over SSH.	SSH IETF RFC 4251
Network Management System (NMS)	The NMS is an external system that can be used to administer and operate the TOE via the Remote Management Interface. NMS communicates with the NE through SNMPv3, SFTP (over SSH v2), NTP and HTTPS. SFTP allows to upload software, perform Database backups from the NMS and collect SNMP and audit logs. HTTPS allows equipment management.	SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 SSH IETF RFC 4251 HTTPS IETF RFC 2818
Key Management Tool (KMT)	The KMT is an external system that can be used to administer and operate the transmission encryption configuration of the TOE via the Remote Management Interface. KMT communicates with the NE through SNMPv3.	SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826
SSH client	A SSH v2 client can be used for initial configuration, management and troubleshooting via the Command Line Interface (CLI).	SSH IETF RFC 4251
SFTP server	A SFTP client can be enabled to upload software, perform DB backups from the NMS and collect SNMP and audit logs.	SSH IETF RFC 4251

Environment	Purpose	Applicable Standards
Secured management network	The secured management network provides security services to protect management protocols and their payloads against eavesdropping, modification, spoofing or/and replay attacks. As detailed later in the document, the means put in place for these protections should be commensurate with the value of the TOE and the user data that the TOE protects (SBU, Restricted, …).	Depends on the security services. It could be VPN IPSec, VPN TLS, …

Table 1.3: Non-TOE Components

1.5.1.1 Scope of Evaluation

This section defines the scope of the TOE to be evaluated.

1.5.1.2 TOE Physical Scope

The physical scope of the TOE is made of:

- A 1830 PSS platform composed of a shelf, power supply, fans, card fillers, a front panel and an Equipment Controller (EC)
- A 11QPEN4 encryption card
- An S13X100E encryption card

The testing platform used for the evaluation includes also an 11DPM12 and 8P20 card. These cards do not implement security functions but provides aggregation functionality. They can aggregate different client rate signals into one ODU-2/ODU-4 frame.

The following TOE components are covered by the physical scope. All three of the PSS32/PSS16II/PSS8 platforms are hardware modules with multi-chip standalone embodiments.

TOE Component	Sub-component	Unique Identifier (APN)	Description	Format[a]	Delivery[b]
1830 PSS-32	32EC2E	8DG63583AA	Equipment Controller Secured (PSS-16II/PSS-32)	PP	StC
	11QPEN4	8DG60996AA	Encryption card 10G	PP	StC
	S13X100E	8DG63988AA	Encryption card 100G	PP	StC
	11DPM12	8DG59828AA	Multiplexer card	PP	StC
	8P20	3KC49240AA	Multiplexer card	PP	StC
	10G MR XFP	3AL82045AA	XFP - XI-64.1 Line XFP, 1310nm, medium reach, OTU2	OM	StC
	10GBASE-SR XFP	1AB375380001	XFP - Client XFP short reach, 850nm, 10 GE	OM	StC

TOE Component	Sub-component	Unique Identifier (APN)	Description	Format[a]	Delivery[b]
	fVOA	1AB396080001	fVOA – fast Variable Optical Attenuator	OM	StC
	X8FCLC-L XFP	1AB375380009	XFP I-64.1/8.5GFC IT (8G FC XFP SM)	OM	StC
	X8FCSN-I XFP	1AB375380011	XFP - 8G FC XFP MM	OM	StC
	XL-64TU XFP	3AL81776AA	XFP - DWDM Tunable CT (50GHz 10G XFP)	OM	StC
	SXI64.1 SFP	1AB390930013	SFP - 10GBASE-LR/OTM-0.2 (1310nm)	OM	StC
	SL64TU SFP	3AL82017AB	SFP - Tunable SFP+ w/o WTE (-5/+85)	OM	StC
	eVOA P-SFP	1AB156220001	SFP - Slow electronic Variable Optical Attenuator (Slow eVOA)	OM	StC
	FC/2FC/4FC SFP	1AB379640001	SFP - B&W 1G/2G/4G Fibre Channel DDM 850nm (SN-I)	OM	StC
	1000B-LX SFP	1AB376720002	SFP - GBE LX -40/+85 (B&W 1GbE 1310nm [1000BASE-LX])	OM	StC
	PF	8DG59242**	Power Supply - (-48V DC) PSS-32, 20A	PP	StC
	Shelf	8DG59319AB	PSS-32 Shelf	rack	StC
	User-Panel	8DG59240AB	PSS-32 User Panel	PP	StC
	Security Label Kit	8DG61510AA	Security Label Kit	TL	StC
	CC User Guide	3KC-70745-NBAA-TSZZA	1830 PSS Release 13.1.0 Common Criteria User Guide	PDF	WSD
	Card Fillers	8DG59418AA	Card Fillers (full slot)	PP	StC
	Fan	8DG59243AB	High Capacity Fan (part of CC EAL3 PSS-32 Shelf kit 8DG64092AA)	PP	StC
1830 PSS-8	8EC2E	3KC48910AA	Equipment Controller Secured (PSS-8)	PP	StC
	11QPEN4	8DG60996AA	Encryption card 10G	PP	StC
	S13X100E	8DG63988AA	Encryption card 100G	PP	StC
	11DPM12	8DG59828AA	Multiplexer card	PP	StC
	8P20	3KC49240AA	Multiplexer card	PP	StC
	10G MR XFP	3AL82045AA	XFP - XI-64.1 Line XFP, 1310nm, medium reach, OTU2	OM	StC
	10GBASE-SR XFP	1AB375380001	XFP - Client XFP short reach, 850nm, 10 GE	OM	StC
	fVOA	1AB396080001	fVOA – fast Variable Optical Attenuator	OM	StC
	X8FCLC-L XFP	1AB375380009	XFP I-64.1/8.5GFC IT (8G FC XFP SM)	OM	StC

TOE Com-ponent	Sub-component	Unique Identifier (APN)	Description	For-mat[a]	Deli-very[b]
	X8FCSN-I XFP	1AB375380011	XFP - 8G FC XFP MM	OM	StC
	XL-64TU XFP	3AL81776AA	XFP - DWDM Tunable CT (50GHz 10G XFP)	OM	StC
	SXI64.1 SFP	1AB390930013	SFP - 10GBASE-LR/OTM-0.2 (1310nm)	OM	StC
	SL64TU SFP	3AL82017AB	SFP - Tunable SFP+ w/o WTE (-5/+85)	OM	StC
	eVOA P-SFP	1AB156220001	SFP - Slow electronic Variable Optical Attenuator (Slow eVOA)	OM	StC
	FC/2FC/4FC SFP	1AB379640001	SFP - B&W 1G/2G/4G Fibre Channel DDM 850nm (SN-I)	OM	StC
	1000B-LX SFP	1AB376720002	SFP - GBE LX -40/+85 (B&W 1GbE 1310nm [1000BASE-LX])	OM	StC
	PF	8DG59242**	Power Supply - (-48V DC) PSS-32, 20A	PP	StC
	Shelf	3KC-48901-AA	PSS-8 shelf	rack	StC
	Security Label Kit	8DG61510AA	Security Label Kit	TL	StC
	CC User Guide	3KC-70745-NBAA-TSZZA	1830 PSS Release 13.1.0 Common Criteria User Guide	PDF	WSD
	Card Fillers	8DG59418AA	Card Fillers (full slot)	PP	StC
	Air Filter	3KC49926AA	MA Air Filter	PP	StC
	8FAN	3KC48850AA	PSS8 Fan Tray	PP	StC
1830 PSS-16II	32EC2E	8DG63583AA	Equipment Controller Secured (PSS-16II/PSS-32)	PP	StC
	11QPEN4	8DG60996AA	Encryption card 10G	PP	StC
	S13X100E	8DG63988AA	Encryption card 100G	PP	StC
	11DPM12	8DG59828AA	Multiplexer card	PP	StC
	8P20	3KC49240AA	Multiplexer card	PP	StC
	10G MR XFP	3AL82045AA	XFP - XI-64.1 Line XFP, 1310nm, medium reach, OTU2	OM	StC
	10GBASE-SR XFP	1AB375380001	XFP - Client XFP short reach, 850nm, 10 GE	OM	StC
	fVOA	1AB396080001	fVOA – fast Variable Optical Attenuator	OM	StC
	X8FCLC-L XFP	1AB375380009	XFP I-64.1/8.5GFC IT (8G FC XFP SM)	OM	StC
	X8FCSN-I XFP	1AB375380011	XFP - 8G FC XFP MM	OM	StC
	XL-64TU XFP	3AL81776AA	XFP - DWDM Tunable CT (50GHz 10G XFP)	OM	StC
	SXI64.1 SFP	1AB390930013	SFP - 10GBASE-LR/OTM-0.2 (1310nm)	OM	StC

TOE Com-ponent	Sub-component	Unique Identifier (APN)	Description	For-mat[a]	Deli-very[b]
	SL64TU SFP	3AL82017AB	SFP - Tunable SFP+ w/o WTE (-5/+85)	OM	StC
	eVOA P-SFP	1AB156220001	SFP - Slow electronic Variable Optical Attenuator (Slow eVOA)	OM	StC
	FC/2FC/4FC SFP	1AB379640001	SFP - B&W 1G/2G/4G Fibre Channel DDM 850nm (SN-I)	OM	StC
	1000B-LX SFP	1AB376720002	SFP - GBE LX -40/+85 (B&W 1GbE 1310nm [1000BASE-LX])	OM	StC
	PF	8DG59242**	Power Supply - (-48V DC) PSS-32, 20A	PP	StC
	Shelf	3KC48960AC	PSS-16II shelf	rack	StC
	16UP2	3KC48980AA	User Panel PSS16 Gen2	PP	StC
	Security Label Kit	8DG61510AA	Security Label Kit	TL	StC
	CC User Guide	3KC-70745-NBAA-TSZZA	1830 PSS Release 13.1.0 Common Criteria User Guide	PDF	WSD
	Card Fillers	8DG59418AA	Card Fillers (full slot)	PP	StC
	Air Filter	3KC49926AA	MA Air Filter	PP	StC
	16FAN2	3KC48990AB	PSS16II FAN	PP	StC

Table 1.4: Physical Scope

[a] Format: the format of the subcomponent is one of PP (pluggable-pack), OM (optical-module), TL (tamper-label), PDF (document in portable document format) or rack.
[b] Delivery: the delivery method describes how a subcomponent is delivered and is one of StC (shipped to customer) or WSD (web site download).

After manufacturing and delivery to customer premises, the TOE is verified, initialized and customized by qualified Nokia personnel. It is assumed that the TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access for manipulation.

1.5.1.3 TOE Logical Scope

Large datacenters have evolved over the years to support different types of applications, including legacy. As a result, it is relatively common for several types of protocols, interfaces, and rates to coexist, with demanding networking requirements. Newer applications like virtualization have increased the amount of data traversing the network, as well as the latency demands. In addition to the differences in interfaces and diverse latency and jitter requirements that these applications demand, older systems do not always provide an integrated ability to use Internet Protocol security (IPsec) or Secure Sockets Layer (SSL) encryption at higher layers. This situation is often addressed by using external hardware devices, which may create additional bottlenecks, increase network complexity, and lead to additional costs.

The TOE provides cryptographic algorithms at DWDM line rate speeds (Layer 1) with little additional latency and jitter. The TOE is designed to secure data at the rates required for handling the typical traffic volumes by datacenter applications.

The 1830 PSS also allows the aggregation of client signals over a single fiber strand and splitting the signal via two geographically diverse paths, in order to ensure network resilience. Each of the signals is monitored at the far end so that if there is a loss of the working signal, a switch is made to the protection path in order to protect the service. Even if this functionality against loss of availability is available and meaningful to support stringent SLA requirements, it is not part of the TOE, since this is not considered a security function.

The logical scope of the evaluation comprises the whole 1830 PSS with its 11QPEN4 and S13X100E cards, except following features that are excluded from the evaluation scope but can be used in accordance with environmental security measures:

- NTP server support.

For SSH, HTTPS and SNMP protocols, they are activated and they can be used to manage the TOE, and their cryptography services are inside the scope of the evaluation.

The following features are disabled on the evaluated software release of 1830 PSS:

- RADIUS support; and
- TL1 support.

Even if features inside the TOE scope, that concern local and remote management, secure the access to the TOE, a secured management network can to be used within the system architecture as shown on the following drawing, and the environment can give additional protection to the EMS and the management interface.

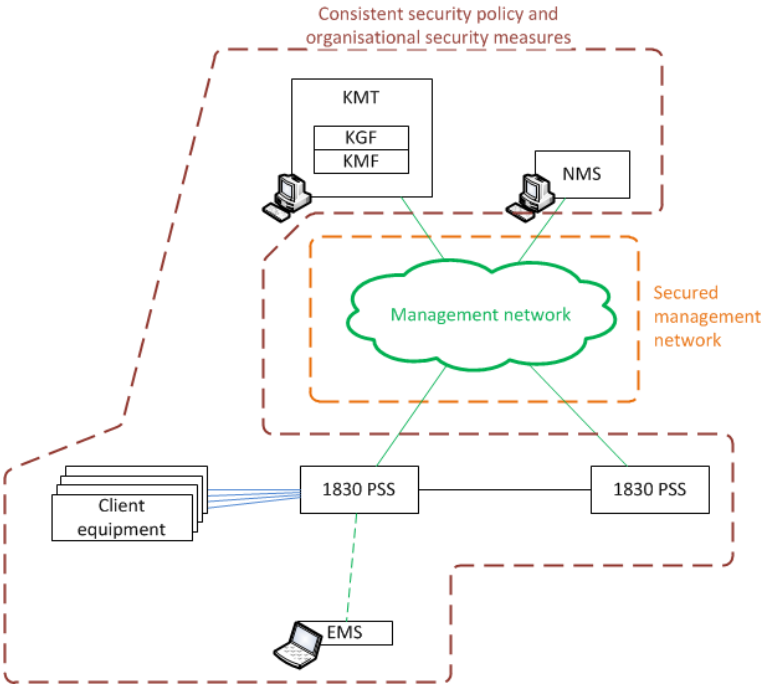


Figure 6 – 1830 PSS Deployment Environment

As the management network (which is part of the TOE environment) transports session keys, it has to be protected in manner commensurate with the value of the TOE and the user data that the TOE protects. At minimum, the secured management network will provide cryptographic support (encryption) or physically secured support. It can also provide integrity, authentication and non-replay security services.
For example, if the network aims to be compliant with the ANSSI “Qualification Standard” [QSTD] requirements, the management network has to be protected in confidentiality, integrity, authentication and non-replay using encryption devices (e.g. VPN IPSec appliances) which are certified and approved by ANSSI.

1.5.1.4 External TOE Physical Interfaces

The TOE provides following physical interfaces available on the Equipment Controler (EC) and on the Encryption cards 11QPEN4/S13X100E:

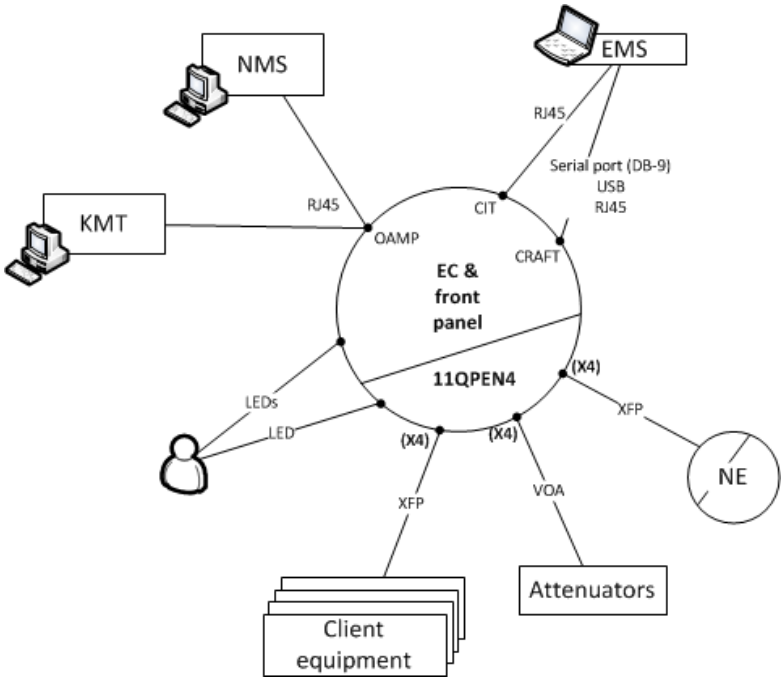


Figure 7 – TOE physical interfaces case 11QPEN4

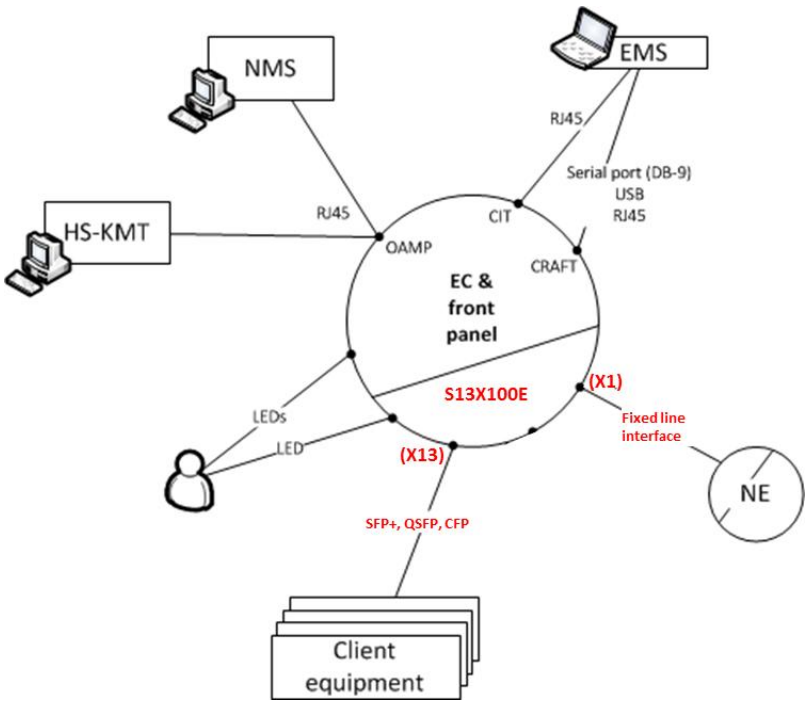
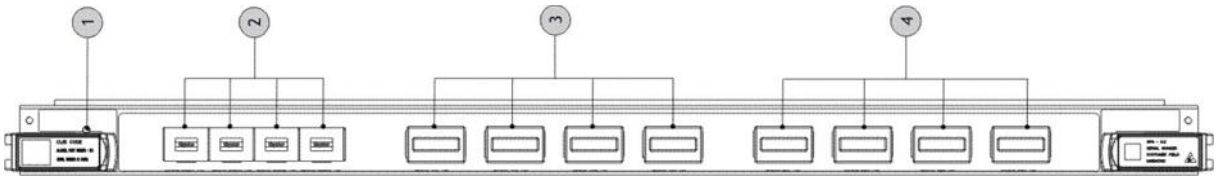


Figure 8 – TOE physical interfaces case S13X100E

The physical interfaces of the TOE are:

- On the 11QPEN4 card:
  - 4 XFP interfaces (client ports) to connect external client equipment
  - 4 XFP interfaces (line ports) to connect the TOE to similar neighboring equipment
  - 4 VOA (Variable Optical Attenuator) sockets to provide a means to optically attenuate the line port signals (one per line port): they do not access or modify the content of the line port signals.
  - A LED to show to an external user nearby the TOE the status of the card



Legend:
1 LEDs "STATUS"
2 VOA1-VOA4 interfaces
3 L1-L4 interfaces
4 C1-C" interfaces

Figure 9 – 11QPEN4 encryption card

- On the S13X100E card:
  - 10 SFP+ interfaces (10G client ports) to connect external client equipment
  - 2 QSFP+ interfaces (40G client ports) to connect external client equipment
  - 1 CFP4 interface (100G client port) to connect external client equipment
  - 1 100G Coherent line interface to connect the TOE to similar neighboring equipment

- A LED to show to an external user nearby the TOE the status of the card

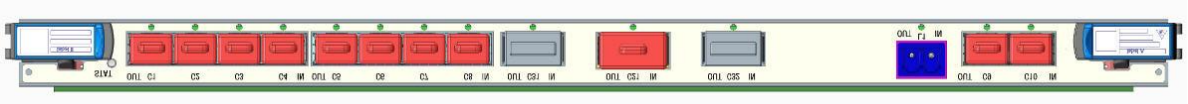


Figure 10 – S13X100E encryption card

- On the controller system
  - Management interfaces to configure and manage the TOE via external equipment:
    - CRAFT (for local management through the EMS) provides CLI over DB-9 port (for PSS-32) and RJ45 port (for PSS-8)
    - CIT (Craft Interface Terminal) for local management through the EMS, which provides CLI over SSH. The CIT is a RJ45 port
    - OAMP (Operation, Administration, Management Port) interface, for remote management through
      - The NMS
      - And the KMT for traffic key generation and import
  - E1 and E2 ports are LAN extension subrack connections, only used in multishelf configurations. (this configuration is outside the scope of the evaluation)
  - VoIP interface allows a Voice over IP connection for offices where telephone service is not available
  - LEDs to show to an external user nearby the equipment the status of the TOE
  - HOUSEKEEPING (connected to a set of relays and input sensors of customer provisionable external items like “central office door half closed”, turn on maintenance pump, etc.)
  - ALARM
  - RACK LAMP

Any other physical interfaces (AUX) are disabled and cannot be used:

- AUX port is an auxiliary interface for further capabilities (not available in the evaluated configuration)

Following drawings shows physical interface per version (1830 PSS-32 / PSS-16II / PSS-8) on the controller system.

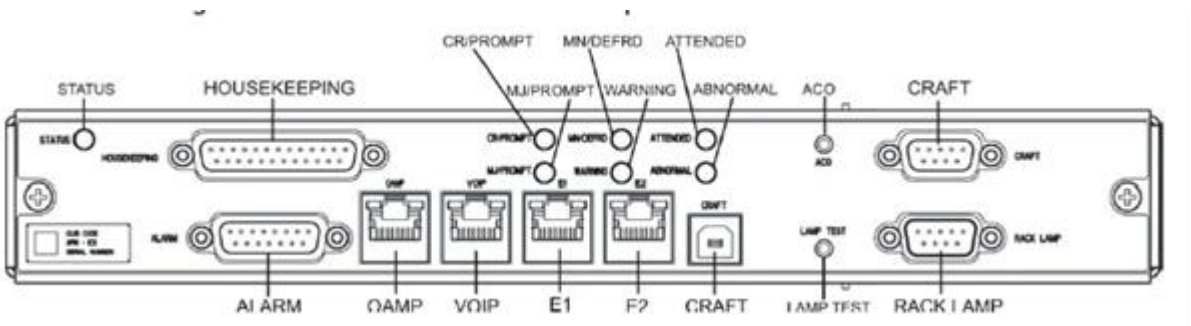


Figure 11 – 1830 PSS-32 front panel

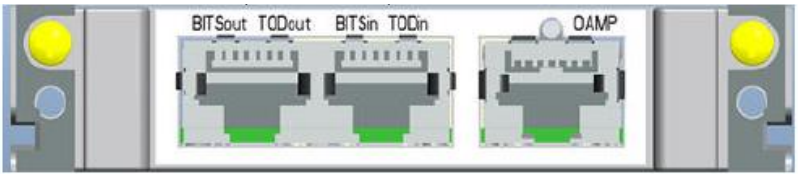


Figure 12 – 1830 PSS-8 front panel

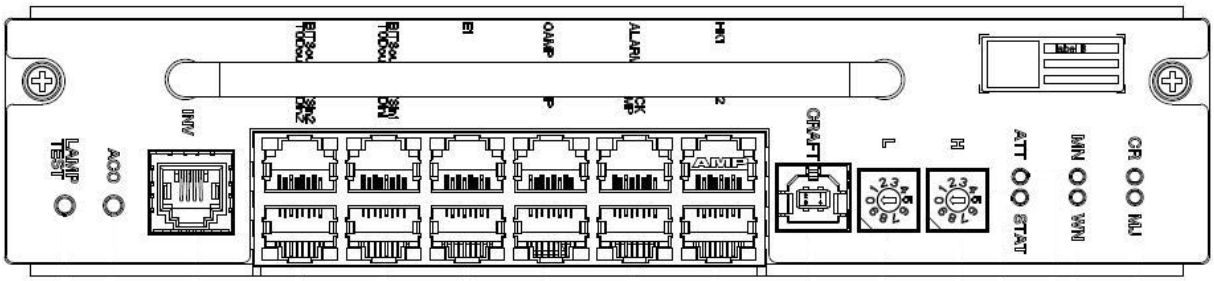


Figure 13 – 1830 PSS-16II front panel

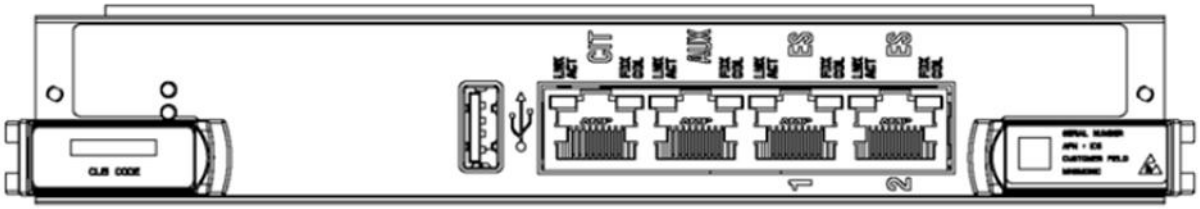


Figure 14 – 1830 PSS-32/PSS-16II EC card

Figure 15 – 1830 PSS-8 EC card

1.5.1.5 External TOE Logical Interfaces

The logical interfaces of the TOE are:

- The data interfaces available for client equipment, which support 8G/10G fiber channel, 10G Ethernet interface (10GE) and Optical Transport Unit 2 (OTU2) on the 11QPEN4 or 10G/40G/100G Ethernet interfaces (10GE/40GE/100GE) and Optical Transport Unit 2/4 (OTU2/OTU4) on the S13X100E.
  The external client data interfaces are connected on a trusted or internal network. Traffic transmitting through the client-side data interfaces is, from the TOE point of view, not encrypted.

- The optical fiber interfaces, which connect the TOE to similar neighboring equipment (systems located on a trusted or internal network) using OTU2 or OTU4 protocol. The payload of the protocol is encrypted by the TOE.
  The fibers between the systems extend through an untrusted or public network.
- Local management interface providing an EMS with TOE management through:
  - CLI over Serial port
  - CLI over SSH
- Remote management interface that provides KMT and NMS with:
  - TOE management through SNMPv3
  - TOE Equipment management through HTTPS for NMS
  - Time management though NTP
  - SFTP (FTP over SSH) for software update and database backup and restore capabilities
  - CLI over SSH

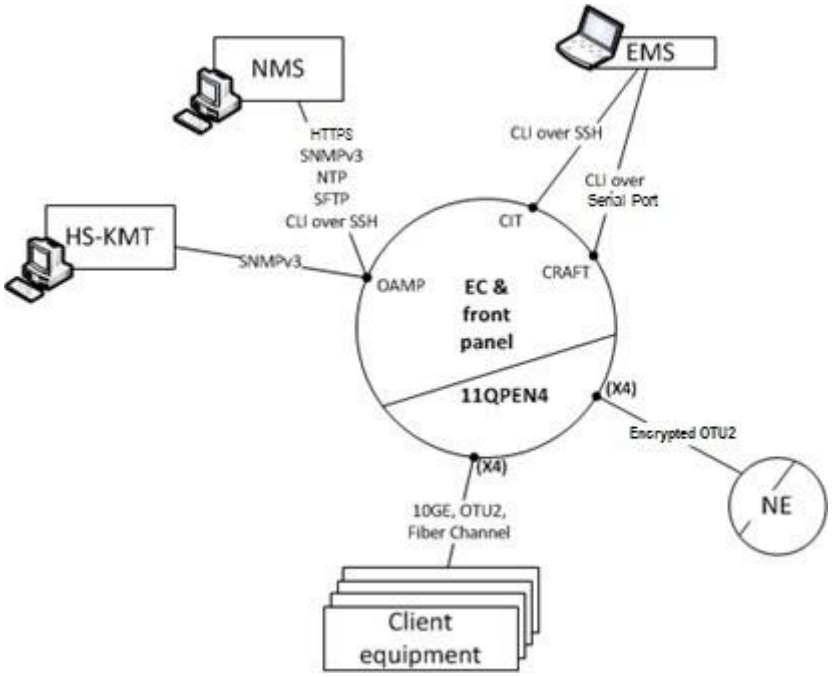


Figure 16 – TOE communication protocols case 11QPEN4

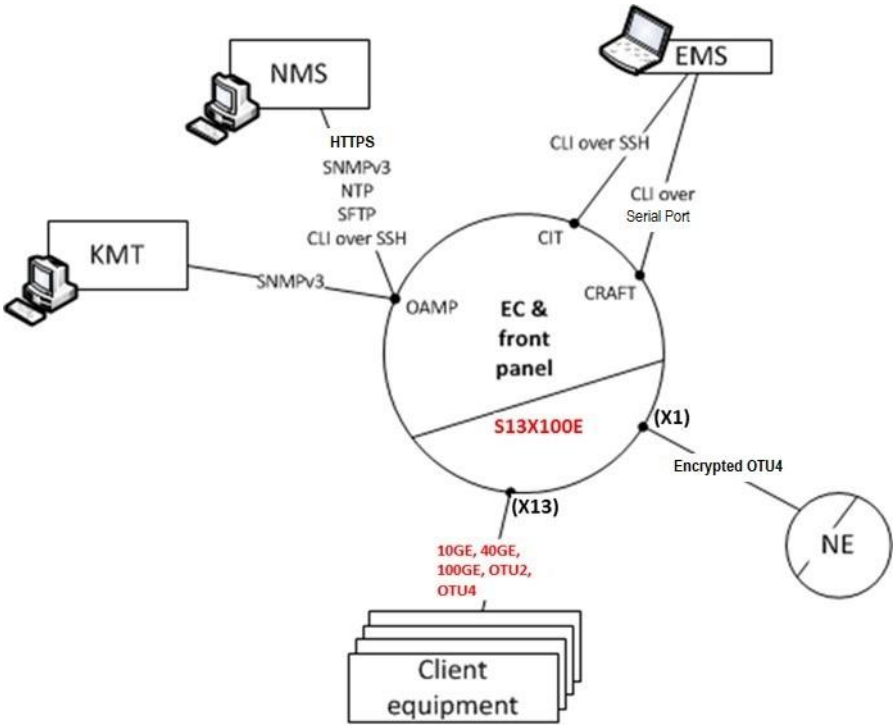


Figure 17 – TOE communication protocols case S13X100E

1.5.2 Summary of Security Features

The TOE comprises the following security features:

- Layer 1 transport protocol encryption
- Secure management
- User identification and authentication
- Potential intrusion alarms
- Self-testing

1.5.2.1 Layer 1 transport protocol encryption

The TOE provides protection against loss of confidentiality along the fiber through layer 1 encryption. It protects OTU-2 lines using AES-256-GCM with 256 bit-keys by means of the 11QPEN4 card or OTU4 lines using AES-256-GMAC with 256 bit-keys by means of the S13X100E card. On the 11QPEN4, each of the four separated optical fiber interfaces uses a different cryptographic key provided by the KMT.

Note: encryption at layer 1 allows independence in the selection of protocols or applications used at higher layers, as well as lower encryption latency than that possible with higher level protocols of the TCP/IP and OSI stacks.

1.5.2.2 Secure Management

The TOE is managed through its Equipment Controller (EC) board. It can be either locally or remotely managed.

For local management, the TOE provides two physical interfaces: a serial port and an Ethernet management interface. A Command Line Interface (CLI) is available on both interfaces.

For remote management, the TOE provides encrypted interfaces for SNMPv3 management functions accessed via a physical Ethernet management interface for KMT and NMS.
The NMS and/or KMT system in the operational environment provides a user friendly interface for the SNMP interface to the TOE. The user can view audit records as they are received by the NMS or KMT system.
For remote management, the TOE provides encrypted interfaces via HTTPS for management functions to handle equipment, accessed via a physical Ethernet management interface for NMS.
The NMS system in the operational environment provides a user friendly interface for the HTTPS interface to the TOE. The user can view audit records as they are received by the NMS system.

The EC provides a secure access to TOE management functionalities (see next subsection for details). For local management, the user shall logon using an individual account. For remote management, authentication is performed through SNMPv3.

For local management, the TOE supports different user roles (Role Based Access Control, RBAC). Roles can be assigned to users by an Administrator using the CLI. Roles determine privileges assigned to users accessing the TOE via the CLI and SNMP. The TOE supports following roles:

- Administrator
- Crypto officer

For remote management, the TOE supports NMS and KMT “roles”. The two equipment are distinguished through their IP address and the cryptographic keys used to protect SNMPv3 protocol. The keys (AuthKey and PrivKey) are configured during system commissioning. The initial configuration of the keys for the Management Interface is done offline and using pre-shared keys. SNMPv3 is configured both as server (for commands) and client (for notifications) in AuthPriv mode.
For remote management of equipment functions, the TOE supports NMS “roles”. The role “Administrator” is used for NMS. The username and password are configured during system commissioning. The initial configuration of username and password for the Management Interface is done offline.

In order to reduce the attack surface of the TOE, other management interfaces available by default and not listed above are disabled, as well as software debug functions and several underlying services of the embedded Operating System. In-band management interfaces and DWDM control plane functions are blocked as part of the TOE.

Role	Privileges
Administrator	This role is the administrator of the TOE. It provides all services that are necessary for initial installation and further management of the module. This role can configure the system and perform provisioning and testing of all IO cards, ports, interfaces, and circuits. It can also create, delete, and modify user accounts. A summary of what this role can do is: - provision the TOE; - configure IO cards, ports, interfaces and circuits; - SNMP configuration;

Role	Privileges
	- defining the external IT entity to which audit data is transferred - management of encryption state and cryptographic parameters for SNMP, SSH (including SFTP); - management of KMT server connection information; - management of system-wide tests; - management of timestamps; - MIB backup and restore; - initiate transfer of non-security related files to RFS, e.g. PM log - execute accessible/privileged TOE command language requests; - TOE software update - Supervise and manage Security Auditing Alarms; - retrieve audit logs; - inhibit and allow all users, including Service user; - manage and retrieve security information about users (not password) such as authentication failure lockout, session inactivity timeout, minimum password length; - obtain user information about the users currently logged on to the TOE (including users that are logged in with NMS or KMT sessions as applicable), Note: SNMP is a session-less protocol; - retrieve information about authenticated (logged on) and unauthenticated (not logged on) sessions; - create and manage traffic circuits between the TOE and other NEs.
Crypto Officer	This role is the administrator for the cryptographic keys. It can manage cryptographic functions and parameters. A summary of what this user can do is: - establish a session with the TOE (logon); - set encryption state and encryption keys; - obtain own user info; - retrieve system-wide user security attributes.
NMS[1]	This role is equivalent to the “Administrator” role. It has access to the same functionalities as the latter except management of users: NMS role can only retrieve information about users, but it can neither create nor modify users and user attributes.
KMT	This role is equivalent to the “Crypto Officer” role. It has access to the same functionalities as the latter.

Table 1.*5: User Roles*

Date and time are configured by the “Administrator” or the “NMS” role, or they can be also synchronized via NTP protocol.

1.5.2.3 User Authentication, Authorization and Audit Logs

The access to management functions is only possible after successful user authentication and authorization. The TOE supports identity-based authentication. Users are identified and authenticated against the local database in the evaluated configuration.

[T]In the remainder of the ST, the “Administrator” role has the same privileges / permissions as the “NMS” role (except about user attributes creation and modification). When the “Administrator” role is mentioned, it is also referring to the “NMS” role.

After users are successfully authenticated to the TOE and authorized according to their assigned role, they may change the system or network configuration.

The following table summarizes authentication mechanism for each role or entity:

Role or entity	Authentication mechanism
Administrator	Password
Crypto Officer	Password
NMS[2]	Password for HTTPS. Authentication symmetric key of the AuthPriv mode of SNMPv3 Note: the key is different from the KMT one.
KMT	Authentication symmetric key of the AuthPriv mode of SNMPv3 Note: the key is different from the NMS one.

Security-related auditable events are recorded in:
- the SNMP log;
- or in the security event log;
- or the User Activities Log (UAL).

These logs can be retrieved using the SFTP protocol for further manipulation and investigation. SNMP is used to automatically transfer these logs to the NMS or KMT system in the operational environment for storage and review.
The TOE will transmit audit records sent to the SNMP log and security event log to an external IT entity using SNMP v3. The audit records are usually sent to an NMS or external log server.

1.5.2.3.1 SNMP log

Activities performed via SNMP are collected and stored locally in a user-readable format, along with the time and date of the action, the source IP address, username and the action itself. One entry is captured for each user action through SNMP. The purpose of this log is to provide accountability.

1.5.2.3.2 Security Event Log

The security event log is used to record all important events of the TOE. These events include managing user accounts, modifying settings, exporting audit logs, and user login.

1.5.2.3.3 User Activities Log (UAL)

All user activities done from CLI are recorded in the User Activity Log (UAL), which is in a user-readable format. Each entry in the UAL contains the time and date of the action, the source IP address, the username and the action itself. One entry is captured for each user action through CLI.

[T]In the remainder of the ST, the “Administrator” role has the same privileges / permissions as the “NMS” role (except about user attributes creation and modification). When the “Administrator” role is mentioned, it is also referring to the “NMS” role.

1.5.2.4 Potential Intrusion Alarms

The TOE provides security notifications on detection of a potential intrusion on the optical fiber. This type of detection is generic to DWDM technology and not explicitly related to security. In a security purpose, a possible scenario is the detection of a Threat Agent disturbing the optical transmission in order to hide an ongoing attack against the fiber or the Neighboring Equipment.

1.5.2.5 Self-tests

Self-tests allow to validate that the TOE runs its security functions properly. These tests are done at TOE power on. The TOE performs validation of the integrity of the software and validation of the cryptographic algorithms.
These tests are run automatically. During their execution, all traffic through the data input and data output ports is inhibited.
The integrity of the software is checked by the Equipment Controller (EC) using a cryptographic hash function.
After software integrity tests and initialisation, cryptographic algorithm tests are performed but each card. These tests are operated through Well Known Answer Tests (WKATs). For traffic encryption algorithm, tests are done by each 11QPEN4 line card for each FPGA and by each S10X100E line card for the ASIC. For software update signature algorithm, test is done by the EC.

1.5.3 Evaluation Test Platforms

The following platforms are used to test the TOE.

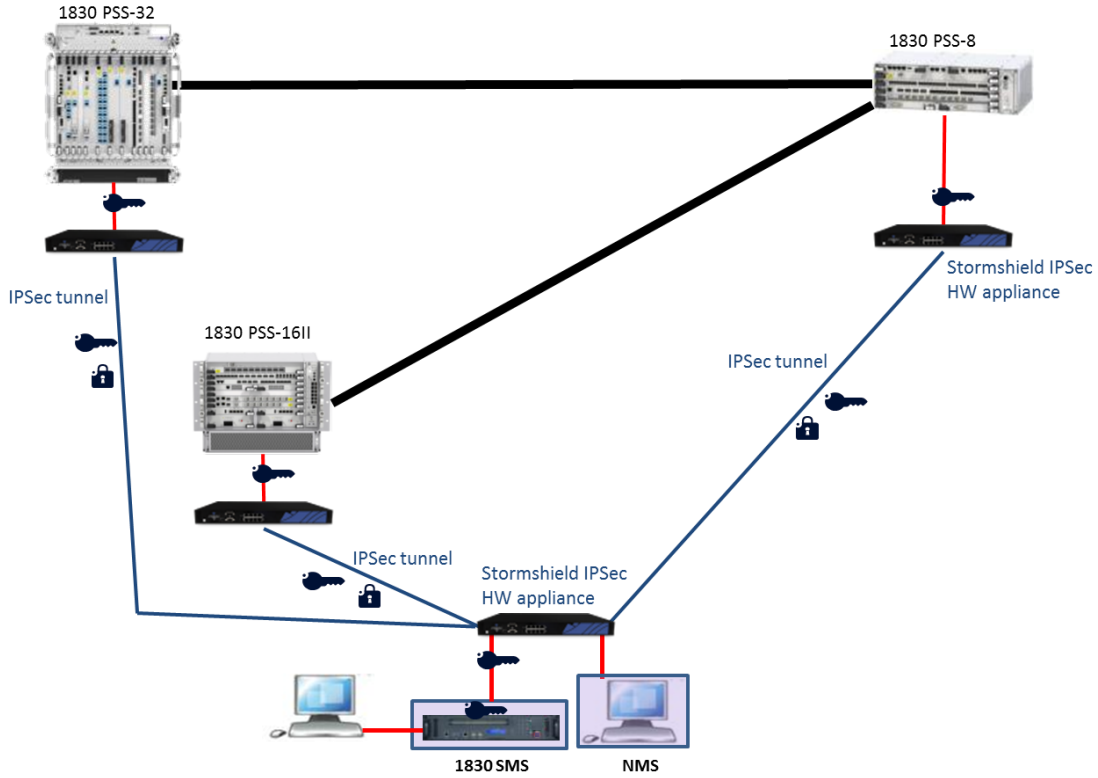


Figure 18 – Evaluation test platform, Physical view

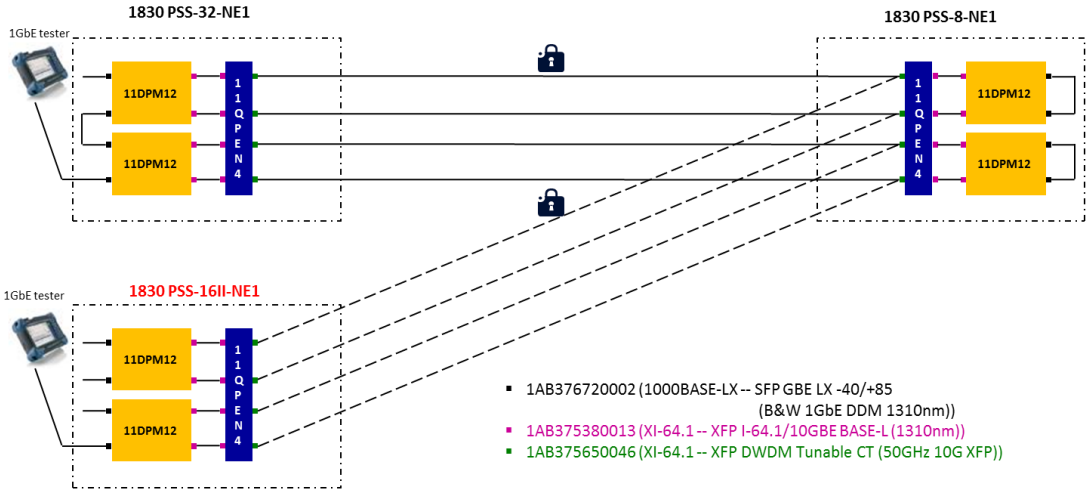


Figure 19 – Evaluation test platform, 11QPEN4 logical view

11DPM12 shall be cascaded with the 11QPEN4 to be used in an ANSSI QS compliant mode: The cascade assures authentication for all encrypted services (see figure above).
8P20 can be used in place of an 11DPM12.

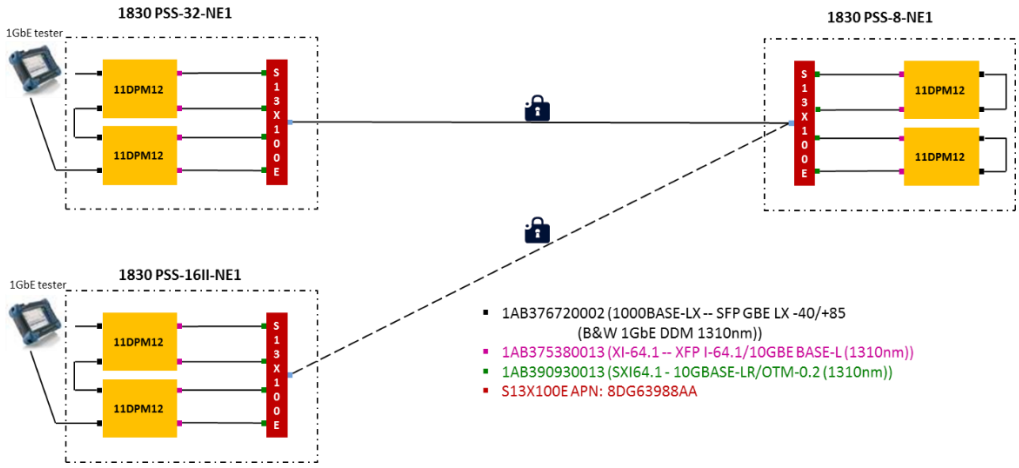


Figure 20 – Evaluation test platform, S13X100E logical view (with 11DPM12)

11DPM12 shall be cascaded with the S13X100E to be used in an ANSSI QS compliant mode: The cascade assures authentication for all encrypted services (see figure above).
8P20 can be used in place of an 11DPM12.

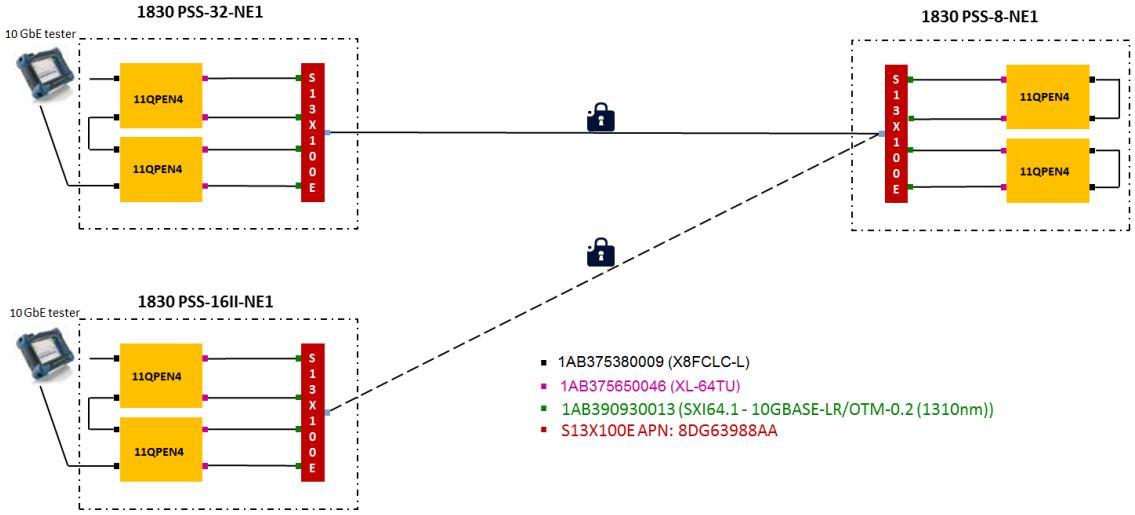


Figure 21 – Evaluation test platform, S13X100E logical view (with 11QPEN4)

11QPEN4 shall be cascaded with the S13X100E to be used in an ANSSI QS compliant mode: The cascade assures authentication for all encrypted services (see figure above).

2. CC Conformance Claim

2.1 CC Conformance Claim

This Security Target claims to be conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [CCP1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [CCP2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [CCP3]

as follows:

- CC Part 2 extended,
- CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 [CEM] has to be taken into account.

2.2 Protection Profile Claim

This Security Target does not claim conformance to a validated Protection Profile.

2.3 Assurance Package Claim

This Security Target claims conformance to Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.3 and AVA_VAN.3.

3. TOE Security Problem Definition

3.1 Assets

This section lists sensitive assets. For each of them, it associates a "security needs" attribute indicating what protection the asset needs.

A security need specified as *optional* means that the risk analysis of the system using the TOE shall determine if this security need is required or not for the purposes of the system. If it is, the user will have to configure the TOE such as it provides the appropriate security protection.

3.1.1 Assets protected by the TOE (User Data)

The primary asset that will be protected by the TOE:

Asset	Definition
D_DATA	User (i.e. client equipment) data in the fiber between the TOE and the neighboring equipment. These data may be temporarily stored in the TOE to be able to process them (i.e., enforce security services) before sending them on to the neighboring equipment. ***Security needs:*** *Confidentiality, Integrity, Authentication, Replay* ***Note:*** *Integrity, Authentication and Non-Replay capabilities are provided by higher level protocols when necessary (by or before the client equipment).*

Table 3.1: TOE Primary Asset

This asset is defined as the data plane by [ITU_2] and is related to the user data transported by the TOE and represents the TOE asset in the sense of the CC.

3.1.2 Assets belonging to the TOE (TSF Data)

The TOE uses secondary assets in order to achieve its security functionalities. They also have to be protected by the TOE in order to support the protection of the primary asset:

Asset	Definition
D_CRYPTO_KEYS	Symmetric keys used by the encryption and decryption of D_DATA. ***Security needs:*** *Confidentiality, Integrity, Authentication, Replay*
D_CONFIG_KEYS	Symmetric and asymmetric keys used for encryption and decryption of D_CONFIG_MANAGEMENT and D_MONITORING_DATA through SNMPv3, SSH, etc. ***Security needs:*** *Confidentiality, Integrity, Authentication, Replay*

Asset	Definition
D_CONFIG_MANAGEMENT	Configuration parameters of the TOE via the management interfaces. This asset groups all TOE configuration parameters that are not confidential ***Security needs:*** *Integrity, Authentication, Replay*
D_AUDIT	This asset represents audit record generated by the TOE: security auditing alarms, SNMP logs, and security event logs generated by the TOE to detect a possible security violation in the equipment or an optical intrusion in the fiber. ***Security needs:*** *Integrity, Authentication, Replay*
D_TIME_BASE	This asset represents the reliable time base kept within the TOE and used by the TOE. ***Security needs:*** *Integrity*
D_MONITORING_DATA	Monitoring data in the out-of-band channel between the TOE and a non-TOE components. Supervision data is data monitored though SNMP request, while other monitoring data is sent by SNMP traps. ***Security needs:*** *Integrity, Authentication, Replay*
D_SOFTWARE_UPDATE	Software update of the TOE. The update is uploaded to the TOE and then installed on the TOE. ***Security needs:*** *Integrity, Authentication*
D_DB_BACKUP	TOE Database backup. ("TOE database" is the implementation in the TOE of the configuration of the TOE.) ***Security needs:*** *Confidentiality, Integrity, Authentication*

Table 3.2: TOE Secondary Assets

These secondary assets are considered part of the management plane as defined by [ITU_2] and represent TSF and TSF-data in the sense of the CC.

3.2 Users

This security target considers the following subjects and descriptions:

Subject	Description
User: Crypto Officer	The Crypto Officer is a user or process authorized to perform self tests, provision and configure the well known answer test (WKAT) and facility information associated with the 11QPEN4 and S13X100E cards, and provision and switch the Encryption Key. The Crypto Officer is a privileged user with Crypto Officer rights defined in Table *1.5*.

Subject	Description
User: Administrator	The Administrator is a user or process authorized to perform configuration and advanced equipment and service management functions. The Administrator is a privileged user with Administrative rights, which include user management as defined in Table *1.5*.
IT Product: NMS	This role is equivalent to the “Administrator” role. It has access to the same functionalities as the latter.
IT Product: KMT	This role is equivalent to the “Crypto Officer” role. It has access to the same functionalities as the latter.
IT Product: EMS	Equipment Management System
Threat Agent	A Threat Agent is a person or process changing the properties of the assets that are part of the TOE. The threat agent may intentionally or unintentionally cause damage. A Threat Agent may also be an attacker with the objective of causing damage or obtaining advantage of D_DATA. The Threat Agent has an Enhanced-Basic (AVA_VAN.3) potential of attack. He has an access to communication links between the TOE and a NE, and between the TOE and the management system (KMT and NMS).

Table 3.3: Subjects

3.3 Threats

T_REMOTE_MNGT

A Threat Agent eavesdrops, intercepts, replays or modifies configuration data or session cryptographic keys between the NMS or KMT and the TOE, resulting in ineffective security mechanisms.

Impacted data:

- D_CRYPTO_KEYS

- D_DATABASE_BACKUP

Impacted security need: *Confidentiality, Integrity, Authentication, Replay*

Impacted data:

- D_CONFIG_MANAGEMENT

Impacted security need: *Integrity, Authentication, Replay*

T_LOCAL_MNGT

A Threat Agent eavesdrops, intercepts, replays or modifies configuration data or session cryptographic keys between the EMS and the TOE, resulting in ineffective security mechanisms.

Impacted data:

- CONFIG_KEYS

- D_DATABASE_BACKUP

Impacted security need: *Confidentiality, Integrity, Authentication, Replay*

Impacted data:

- D_CONFIG_MANAGEMENT

Impacted security need: *Integrity, Authentication, Replay*

T_MALICIOUS_UPDATES

A Threat Agent upload and install a malicious software or modifies a software update before it is uploaded and installed on the TOE, in order to trap and change the behaviour of the TOE.

Impacted data:

- D_SOFTWARE_UPDATE

Impacted security need: *Integrity, Authentication*

T_ADMIN_ERROR

An administrator or a Crypto Officer unintentionally installs or configures the TOE incorrectly, resulting in ineffective security mechanisms.

Impacted data:

- D_CONFIG_KEYS

- D_CONFIG_MANAGEMENT

- D_AUDIT

Impacted security need: *Integrity*

T_TSF_FAILURE

Security mechanisms of the TOE fails, leading to a compromise of TSF Data or User Data that a Threat Agent eavesdrops and retrieves.

Impacted data:

- D _DATA

- D_CRYPTO_KEYS

Impacted security need: *Confidentiality*

T_UNDETECTED_ACTIONS

A Threat Agent takes actions that adversely affect the security of the TOE. He intercepts (and deletes) or modifies audit data or alarms sent by the TOE to the NMS or the KMT, in order to cover up the attack.

Impacted data:

- D_MONITORING_DATA

- D_AUDIT

Impacted security need: *Integrity, Authentication*

T_UNAUTHORISED_ACCESS

A Threat Agent gains unauthorized access to the TOE data and TOE executable code.

A Threat Agent (malicious user, process, or external IT entity) masquerades as an authorized entity in order to gain unauthorized access to data or TOE resources.

A Threat Agent (malicious user, process, or external IT entity) misrepresents itself as the TOE to obtain identification and authentication data.

Those actions could lead either to :

– Modification or retrieval of TOE data (that is TSF Data and User Data persistently stored within the TOE)

– Usurpation of an administrator identity in order to perform administration operations on the TOE

Impacted data:

- D _DATA

- D_CRYPTO_KEYS

- D_CONFIG_KEYS

- D_DB_BACKUP

Impacted security need: *Confidentiality, Integrity*

Impacted data:

- D_CONFIG_MANAGEMENT

- D_TIME_BASE

Impacted security need: *Integrity*

T_TIME_BASE

A threat Agent disturbs or tampers with the TOE time base with the aim of falsifying audit data.

Impacted data:

- D_TIME_BASE

Impacted security need: *Integrity*

T_RESIDUAL_DATA

A Threat Agent acquires knowledge, through direct access to the TOE, of old value of TOE data (keys, configuration…) during a change of operational context (assignment of the TOE in a new premise, maintenance…).

Impacted data:

- D_CONFIG_ MANAGEMENT

- D_CRYPTO_KEYS

- D_CONFIG_KEYS

Impacted security need: *Confidentiality*

3.4 Assumptions

The following assumptions apply to the TOE environment.

A_ORGANIZATION

It is assumed that the organization follows a systematic security standard or management process that ensures that security controls meet the organization security needs and provide an adequate management of security risks, threats, vulnerabilities and their impact.

A_ADMIN

It is assumed that TOE Crypto Officers and TOE Administrators are trusted and well trained.

They apply the procedure described in the administration guide.

A_AUDIT

It is assumed that alarms are monitored and SNMP logs, security event logs and UAL are regularly examined by the TOE Administrators and corrective actions are taken upon potential incident detection according to recommendations for managing the TOE.

A_CONFIGURATION

It is assumed that the TOE is configured following recommendations in order to properly protect the primary and secondary assets of the TOE.

It is assumed that Neighbouring Equipment and non-TOE components, as defined in Table 1.3, are configured following the vendor security recommendations.

A_PROTECTION

It is assumed that:

a) The TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access to the TOE.

b) Neighbouring Equipment have at least the same level of physical and logical protection as the TOE.

c) User data D_DATA (coming from or sent to client equipment) intended for transmission via the TOE are protected.

A_KGF

It is assumed that key generation meets ANSSI guidance [GdMC] regarding key generation. It is CC EAL4+ (AVA_VAN.4) or ANSSI QR certified.

A_MNGT_NETWORK

It is assumed that Management Network which interconnects the KMT, the NMS and the TOE (and its NEs) is a secured network. Security services provided by the secured management network are commensurate with the value of the user data protected by the TOE. They provide protections in confidentiality, integrity, authentication and/or non-replay.

A_MNGT_EQPT_SECURED

It is assumed that following equipment are properly and securely configured, according the sensitivity of assets they handle:

- NMS
- KMT
- EMS

A_MNGT_EQPT_PROTECTION

It is assumed that following equipment have at least the same level of physical and/or logical protection as the TOE:

- NMS
- KMT
- EMS

3.5 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices or guidelines imposed by an organization upon its operations. The OSP are suggested as basic operational practices to be implemented in a properly managed datacenter environment. A datacenter environment, depending on the applications, services and country regulation may have to follow additional operational practices not covered by this list of objectives.

OSP_CRYPTO_RGS

The TOE shall implement cryptographic mechanisms compliant with ANSSI guidance [GdMC].

OSP_ACCESS

The TOE shall provide logical access control mechanisms.

User access to the TOE shall be controlled by a secure authentication and authorization process.

OSP_ALARM

The TOE shall provide security-relevant notifications that support the users to identify potential intrusion events.

OSP_AUDIT

The TOE shall provide audit trails that allow tracking configuration changes to the TOE, since users shall be made accountable for such actions.

OSP_CRYPTO

The TOE shall provide D_DATA encryption and decryption compliant to internationally accepted cryptographic standards.

OSP_MANAGEMENT

The TOE shall provide a management capability for the equipment and its cryptographic functions.

OSP_KEY_MANAGEMENT

The TOE shall provide mechanisms and procedures that allow the KMT to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS.

OSP_ROLES

The TOE shall provide a user management function, which allows the assignment of different levels of authorization for administration and operation.

OSP_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment

4.1 Security Objectives for the TOE

The following TOE security objectives address the protection provided by the TOE independent of the TOE environment.

O_ACCESS

The TOE shall protect against all non-authorized logical access attempts. The TOE shall also provide mechanisms for authenticating Users prior to granting access to those functions which they are authorized to use based upon their assigned role.

O_ALARM

The TOE shall notify the User about the following potential intrusion events via the Management Interface:
a) DWDM Transmission Errors
b) Loss of connection with NMS
c) Loss of connection with KMT

O_AUDIT

The TOE shall record security relevant events, such as TOE configuration changes and DWDM transmission errors.
The TOE must transmit audit data to an external trusted entity for storage and viewing.

The TOE shall associate to generated audit data:
- The date and time of event generation
- A number (an incremental counter), offering a mean to detect audit data loss.
- A severity, offering a mean to discriminate informational, warning and critical audit data.
- A type.

O_CRYPTO_CONFORMITY

The TOE shall provide D_DATA encryption and decryption which conforms to ANSSI requirements [GdMC].

O_DATA_CONFIDENTIALITY

The TOE shall provide encrypted communication between itself and a NE, in order to protect the confidentiality of D_DATA.

O_KEY_MANAGEMENT

The TOE shall provide mechanisms that allow authenticated and authorized users to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS.

O_MANAGEMENT

The TOE shall provide a management capability that allows authenticated and authorized users to manage the equipment and its cryptographic functions.

O_TIME_BASE

The TOE provides a time base upon which the audit records are based and ensures its reliability.

O_SW_UPDATES

The TOE shall check software updates integrity and authentication, prior installing it.

O_ROLES

The TOE shall provide a RBAC mechanism for local management. The user management function allows defining users for operation and administration based on the general privilege categories listed in Table *1*.5.
The roles are :
- Administrator
- Crypto Officer

O_I&A

The TOE shall require the identification of a device before granting it with the NMS or KMT access rights.
The TOE shall require the authentication of the user before granting him with his access rights.
The TOE shall provide means to protect user sessions (session lock and termination, user account blocking).

O_DISPLAY_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

O_SELF_TESTING

The TOE shall run a set of tests at startup.

O_RESIDUAL_INFO_CLEARING

The TOE shall ensure that any D_DATA encryption cryptographic key (that is D_CRYPTO_KEYS) is made unavailable after use.

4.2 Environmental Security Objectives

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment independent of the TOE itself.

4.2.1 TOE Development

OE_GENERAL_PUPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

4.2.2 Organization and TOE Administration

OE_ORGANIZATION

The OE and all employees shall follow the organizational policies, guidelines and procedures, which have been established in regard to the organization security needs and result from an adequate management of security risks, threats, vulnerabilities and their impact.

OE_TRUSTED_ADMIN

The OE shall ensure that users are properly trained to perform TOE tasks according to their role.

In particular, TOE Crypto Officers and TOE Administrators shall be trained to configure and supervise the TOE and its security functions, applying the procedure described in the administration and the user guide.

OE_AUDIT

The OE shall ensure that TOE Users monitor alarms and TOE Administrators regularly reviews SNMP logs, security event logs and UAL.

The TOE Administrators shall also ensure that appropriate corrective actions, according to Nokia recommendations for managing the TOE, are taken upon potential incident detection.

OE_TOE_CONFIGURATION

The OE shall ensure that the TOE and its Neighboring Equipment are installed and commissioned following Nokia recommendations and procedures in order to properly protect user data (D_DATA) and secondary assets of the TOE.

OE_DB_BACKUP

The OE shall preserve database backup integrity and authentication, in order to prevent any malicious modification, trapping and substitution.

4.2.3 Management network

OE_KGF

The key generation shall meet ANSSI requirements [GdMC]. It shall be CC EAL4+ (AVA_VAN.4) or ANSSI QR certified.

OE_MNGT_NETWORK

SSH, HTTPS, SNMP cryptographic support and other management protocols are inside the scope of the evaluation. The communication link between the NMS or the KMT and the TOE (respectively the NE) has to be protected in confidentiality, integrity, authentication and non-replay. In addition security can be increased through a secured management network.

To keep reliability and integrity of the NMS and the KMT, prior to interconnecting it with any network (i.e. management or external network), the OE shall perform a risk analysis and determine necessary security technical and/or organizational measures to put in place between the NMS, the KMT and the networks, commensurate to the value of the TOE and the user data the TOE protects (D_DATA).

For instance, VPN IPSec devices, being approved at ANSSI “Qualification Standard level of security”, may be placed between the NMS (and KMT) and the TOE (respectively the NE). The OE shall ensure that the VPN IPSec device is installed and configured following vendor’s recommendations and procedures in order to properly protect management data (D_CRYPTO_KEYS, D_CONFIG_MANAGEMENT).

OE_LOCAL_MNGT

The OE provides physical and logical protections of the management communication link using the CRAFT and the CIT interfaces commensurate with the value of the TOE and the user data the TOE protects (D_DATA). The OE may perform a risk analysis to determine the appropriate security measures.

Those measures apply to:

– The EMS, which have to be physically and logically secured

– The link between the EMS and the TOE, which integrity has to be preserved

OE_MNGT_EQPT_SECURED

The OE shall ensure that non-TOE components are configured following the vendor security recommendations and settings.

The OE shall ensure that following equipment are properly and securely configured, according the sensitivity of assets they handle:

– NMS

– KMT

– EMS

It is assumed that their operating system is configured accordingly to the appropriate security guidance and that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on those devices, other than services necessary for the operation and support of their functionalities.

In case sensitive data are governmental data at Restricted level of classification (DR, NR, EUR), it is assumed that devices are configured in regard to appropriate rules and regulations.

OE_MNGT_EQPT_PROTECTION

The OE shall ensure that following equipment have at least the same level of physical and/or logical protection as the TOE:

– NMS

– KMT

– EMS

The overall solution allows individual access accounting (e.g. physical access restriction to the device hosting the software, user authentication by the operating system, etc.)

OE_SECONDARY_ASSETS_PROTECTION

It is also assumed that non-TOE management assets and the defined secondary assets have at least the same level of physical and/or logical protection as the TOE.

4.2.4 Protections

OE_TOE_PROTECTION

The OE shall ensure that the TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access.

The Neighboring Equipment shall have at least the same level of physical and logical protection as the TOE.

OE_DATA_PROTECTION

The OE shall protect data intended for transmission to the TOE (that is D_DATA).

The OE shall handle data originating from the TOE securely.

4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

		O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_KEY_MANAGEMENT	O_MANAGEMENT	O_TIME_BASE	O_SW_UPDATES	O_ROLES	O_I&A	O_DISPLAjY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING	OE_GENERAL_PUPOSE	OE_ORGANIZATION	OE_TRUSTED_ADMIN	OE_AUDIT	OE_TOE_CONFIGURATION	OE_DB_BACKUPS	OE_KGF	OE_MNGT_NETWORK	OE_LOCAL_MNGT	OE_MNGT_EQPT_SECURED	OE_MNGT_EQPT_PROTECTION	OE_SECONDARY_ASSETS_PROTECTION	OE_TOE_PROTECTION	OE_DATA_PROTECTION
Threats	T_REMOTE_MNGT		X	X																			X		X	X		X	
	T_LOCAL_MNGT			X																				X	X	X		X	
	T_MALICIOUS_UPDATES			X						X																			
	T_ADMIN_ERROR			X														X											
	T_TSF_FAILURE													X															
	T_UNDETECTED_ACTIONS			X																			X		X	X			
	T_UNAUTHORISED_ACCESS	X	X	X				X			X	X											X	X	X	X			
	T_TIME_BASE								X																				
	T_RESIDUAL_DATA														X														
Assumptions	A_ORGANIZATION																X												
	A_ADMIN																	X											
	A_AUDIT																		X										
	A_CONFIGURATION																			X					X				
	A_PROTECTION																				X						X	X	X
	A_KGF																					X							
	A_MNGT_NETWORK																						X						
	A_MNGT_EQPT_SECURED																							X					
	A_MNGT_EQPT_PROTECTION																								X				

		O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_KEY_MANAGEMENT	O_MANAGEMENT	O_TIME_BASE	O_SW_UPDATES	O_ROLES	O_I&A	O_DISPLAjY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING	OE_GENERAL_PUPOSE	OE_ORGANIZATION	OE_TRUSTED_ADMIN	OE_AUDIT	OE_TOE_CONFIGURATION	OE_DB_BACKUPS	OE_KGF	OE_MNGT_NETWORK	OE_LOCAL_MNGT	OE_MNGT_EQPT_SECURED	OE_MNGT_EQPT_PROTECTION	OE_SECONDARY_ASSETS_PROTECTION	OE_TOE_PROTECTION	OE_DATA_PROTECTION
OSPs	OSP_CRYPTO_RGS				X																		X						
	OSP_ACCESS	X																											
	OSP_ALARM		X																										
	OSP_AUDIT			X																									
	OSP_CRYPTO				X	X																							
	OSP_MANAGEMENT							X			X	X																	
	OSP_KEY_MANAGEMENT						X																X		X	X	X		
	OSP_ROLES										X																		
	OSP_BANNER												X																

Assumption, Threat or OSP	Rationale
A_ADMIN	OE_TRUSTED_ADMIN requires the operational environment to ensure that users are properly trained to perform TOE tasks according to their role as assumed by A_ADMIN. Furthermore OE_TRUSTED_ADMIN particularizes the training concepts for administrators and crypto officers.
A_AUDIT	OE_AUDIT requires the user to monitor alarms and an administrative user to regularly review SNMP Logs,security event logs and UAL,as assumed in A_AUDIT. Also OE_AUDIT requires that appropriate corrective actions, according to Nokia recommendations for managing the TOE are taken upon potential incident detection as assumed in A_AUDIT.
A_GENERAL_PUPOSE	OE_GENERAL_PUPOSE requires no other services available on the operating system of the TOE other than those necessary for the operation and management. In particular it requires no general-purpose computing capabilities.
A_CONFIGURATION	OE_TOE_CONFIGURATION covers what is assumed in A_CONFIGURATION, since it requires that the TOE and Neighboring Equipment areinstalled and commissioned following Nokia recommendations and procedures in order to properly protect the primary and secondary assets of the TOE. In addition, OE_MNGT_EQPT_SECURED requires that non-TOE components are configured following the vendor security recommendations and settings.
A_ORGANIZATION	OE_ORGANIZATION requires the operational environment and employees to follow organizational policies, guidelines and procedures as assumed in A_ORGANIZATION.
A_PROTECTION	OE_TOE_PROTECTION requires that the TOE and the Neighboring Equipment are located in a controlled and secured zone in order to prevent unauthorized logical and physical access. OE_SECONDARY_ASSETS_PROTECTION requires that non-TOE management assets have at least the same level of physical and logical protection as the TOE. Specifically, OE_DB_BACKUPS requires that database backups are securely handled in order to preserve their integrity. Furthermore, OE_DATA_PROTECTION requires that data intended for transmission to the TOE including D_DATA is protected.
A_KGF	OE_KGF requires a key generation functionality compliant with ANSSI requirements regarding cryptography, stated within [GdMC].
A_MNGT_NETWORK	OE_MNGT_NETWORK requires a risk analysis to determine how secure should be the management network. In order to use the TOE in a context compliant with a “Qualification Standard” level of security, OE_MNGT_NETWORK recommends using ANSSI approved IPSec encryption devices for additional security.
A_MNGT_EQPT_SECURED	OE_MNGT_EQPT_SECURED requires management devices and subsystems to be secured following the vendor security recommendations and settings. Their operating system should be secured.accordingly to applicable security or governmental recommendations depending on the system that uses the TOE.

Assumption, Threat or OSP	Rationale
A_MNGT_EQPT_PROTECTION	OE_MNGT_EQPT_PROTECTION requires physical and logical protection for management devices and subsystems, at least at the same level of protection as the TOE. Furthermore, it requires the overall solution to allow individual access accounting to access those devices.
T_REMOTE_MNGT	Due to the evaluation scope, the threat is countered by built-in and environmental measures. The remote management network is recommended to be secured by the environment (OE_MNGT_NETWORK). A risk analysis determines the technical and organisational means and measures. Nearby the TOE, the remote management link is protected by the organisational measures protecting the TOE itself (OE_TOE_PROTECTION). Furthermore, management subsystems (NMS and KMT) shall be protected too (OE_MNGT_EQT_PROTECTION), and their platform shall be properly secured (OE_MNGT_EQT_SECURED). O_AUDIT supports the OE by requiring event record generation for any management operation, and O_ALARM requires the TOE to warn the user when connection is lost with NMS or KMT.
T_LOCAL_MNGT	Due to the evaluation scope, the threat is countered by environmental measures. The local mangement interfaces and communication link are protected thanks to the organisational measures protecting the TOE itself (OE_LOCAL_MNGT and OE_TOE_PROTECTION) Furthermore, management device (EMS) shall be protected too (OE_MNGT_EQT_PROTECTION), and its platform shall be properly secured (OE_MNGT_EQT_SECURED). O_AUDIT supports the OE by requiring event record generation for any management operation.
T_MALICIOUS_UPDATES	This threat is countered by O_SW_UPDATES which requires the TOE to check integrity and authentication of software updates prior to install it, and by O_AUDIT which requires event record generation for security events (software updating is a security event).
T_ADMIN_ERROR	This threat is countered by OE.TRUSTED_ADMIN which ensures that administrators (U.LOCAL_ADMINISTRATOR and U.CENTRAL_ADMINISTRATOR) apply all guidance in a trusted manner. O.AUDIT contributes to the threat coverage by providing audit data generation for all operations (including viewing operations on TOE sensitive assets) performed by the administrators.
T_TSF_FAILURE	This threat is countered by O.SELF_TEST which requires checking ot the integrity of the software which enforces security.
T_UNDETECTED_ACTIONS	This threat is covered by O.AUDIT, which requires the TOE to generate audit for security-relevant operations performed by the TOE or concerning protected communication channels, and for actions performed by users. Security objectives for the environment support O.AUDIT by requiring secure management network, secured management devices and a secured SNMPv3 and SSH link: OE_MNGT_NETWORK, OE_MNGT_EQPT_SECURED, OE_MNGT_EQPT_PROTECTION.

Assumption, Threat or OSP	Rationale
T_UNAUTHORISED_ACCESS	The threat is countered by O.MANAGEMENT which requires that management can only be done by authorised entities This security objectives relies on identification & authentication: - O_ACCESS and O_I&A which requires the user to be authenticated before performing any management functions based upon their roles (O_ROLES). Protection of TOE local management communication is ensured through OE_LOCAL_MNGT, as management through CRAFT and CIT ports is considered in clear text, whatever is the protocol (CLI over serial port, CLI or FTP over SSH, etc.), due to the evaluation scope. - OE_MNGT_NETWORK which requires a secured remote management network commensurate to the overall security determined through a risk analysis. - OE_MNGT_EQPT_SECURED and OE_MNGT_EQT_PROTECTION which require protection of management devices and subsystems. The following objectives also contribute to the threat coverage: - O.ALARM requiring the TOE to emit an alarm in case of potential intrusion detection. - O.AUDIT ensures that operations (viewing, modification) performed on TOE sensitive assets are logged and that critical security events are generated to indicate TOE operational failures. Therefore, they provide the capability to detect and process errors or attacks after an analysis of audit events and security alarms.
T_TIME_BASE	This threat is covered by the security objective O_TIME_BASE which ensures the time base reliability.
T_RESIDUAL_DATA	This threat is countered by O.RESIDUAL_INFO_CLEARING to ensure that no unused user data remains in TOE's volatile memory.
OSP_CRYPTO_RGS	O_CRYPTO_CONFORMITY requires Layer 1 protection that complies to ANSSI requirements [GdMC]. Furthermore, for governmental use and depending on the risk analysis for the management network, O_MNGT_NETWORK requires, should they be deployed, VPN IPSec devices conformant to ANSSI “Qualification Standard” security level.
OSP_ACCESS	O_ACCESS requires the TOE to be protected against non-authorized logical access and to provide mechanisms for authenticating users before granting access to the functions that they have been specifically authorized to use. So, an access control mechanism for the TOE is needed. OSP_ACCESS exactly requires a logical access control mechanism. Also, it requires TOE access that is controlled by a secure authentication and authorization process. O_ACCESS likewise requires a secure authentication and authorization process.
OSP_ALARM	OSP_ALARM requires the TOE to provide security-relevant notifications that support the users to identify potential intrusion events. Therefore, it is covered by the objective O_ALARM which requires the TOE to notify users about potential intrusions (DWDM transmission errors).
OSP_AUDIT	Since O_AUDIT requires the TOE to provide SNMP Logs, security event logs and user activity logs that allow tracking configuration changes to the TOE. It also requires that audit records are sent to an external IT entity for storage and viewing.

Assumption, Threat or OSP	Rationale
OSP_CRYPTO	O_DATA_CONFIDENTIALITY requires the TOE to provide conformity for D_DATA encryption and decryption. O_CRYPTO_CONFORMITY requires the TOE to provide crypto services conformant to ANSSI requirements [GdMC] which accepts internationally recognize cryptographic algorithms.
OSP_MANAGEMENT	O_MANAGEMENT requires the TOE to provide a management capability that allows authenticated and authorized users (through O_I&A and O_ROLES) to manage the equipment and its cryptographic functions.
OSP_KEY_ MANAGEMENT	O_KEY_MANAGEMENT exactly requires the provision of mechanisms that allow authenticated and authorized users to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS. The environment shall maintain their security through procedural and technical means (OE_MNGT_NETWORK, OE_MNGT_EQPT_SECURED, OE_MNGT_EQPT_PROTECTION, OE_SECONDARY_ASSETS_PROTECTION)
OSP_ROLES	O_ROLES requires a role management function which allows defining users for operation and administration based on the general privilege categories “crypto officer and administrator”.
OSP_BANNER	O_DISPLAY_BANNER requires the TOE to display a banner at user login to describe restrictions of use and legal agreements by accessing the TOE.

Table 4.1: Security Objective Rationale

5. Extended Components Definition

5.1 Extended TOE Security Functional Family

This Security Target defines new security functional families, which are used to define the security requirements for this ST.

5.1.1 FPT_TUD_EXT – Trusted Update

The FPT_TUD_EXT family, defines requirements for software update and integrity.

5.1.1.1 Definition

Family Behaviour

This family FPT_TUD_EXT (Trusted Update) extends the functional class FPT with the capability to update TSF firmware/software parts.

Component levelling

FPT_TUD_EXT.1 Trusted Update, requires the TSF to provide a trusted firmware/software update mechanism.

Management: FPT_TUD_EXT.1

There are no management activities foreseen.

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Initiation of update.

FPT_TUD_EXT.1	**Trusted Update**
	Hierarchical to: No other components.
	Dependencies: FCS_COP.1 Cryptographic operation
FPT_TUD_EXT.1.1	The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a [selection: digital signature mechanism, published hash] prior to installing those updates.

5.1.1.2 Rationale

This family was defined because part 2 of [CC] does not contain any SFR which allows specifying requirements about trusted firmware/software update.

5.2 Extended TOE Security Functional Components

This Security Target defines new security functional components, which are used to define the security requirements for this ST.

5.2.1 FAU_STG

The FAU_STG family, as defined in CC Part 2, defines requirements for creating, maintaining and storing a security audit trail.

5.2.1.1 FAU_STG_EXT

FAU_STG_EXT.1 External Audit Trail Storage specifies that audit records can be transmitted to an external IT entity using a trusted channel.

Management FAU_STG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuring and maintaining the external IT entity to which the TSF sends the audit records.

Audit: FAU_STG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Modifying the external IT entity to which the TSF sends the audit records.

FAU_STG_EXT.1	**External Audit Trail Storage**
	Hierarchical to: No other components.
	Dependencies: FAU_GEN.1 Audit data generation
FAU_STG_EXT.1.1	The TSF shall be able to [selection: transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity] using a trusted channel implementing the [selection: Ipsec, SSH, SNMPv3] protocol.

5.2.1.2 Rationale

This family was defined because part 2 of [CC] does not contain any SFR which allows transmitting audit trail to an external storage capability. For the TOE described in this ST it was necessary to provide such capability.

5.3 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6. Security Requirements

6.1 Security Functional Requirements

The following format will be used to represent assignment, selection, refinement and iteration operations:

- An assignment operation will be identified as normal text in square brackets.
  - [value_1, value_2]
- A selection operation will be identified as italic text in square brackets.
  - [*value_1, value_2*].
- An assignment operation inside a selection operation will be identified as bold italic text in square brackets.
  - [*value_1,* ***value_2****, value_3*]
- A refinement operation will be identified as bold text for when new text has been inserted into the security functional requirement and strikethrough text will be used when text has been deleted.
  - original_text_1 **new_text** original_text_2 ~~removed_text~~ original_text_3
- An iteration of a security functional requirement will be identified by appending an additional identifier in round brackets next to their original identifier.
  - FCS_COP.1(1).

6.1.1 Security Audit (FAU)

FAU_ARP.1	**Security alarms**
FAU_ARP.1.1	The TSF shall ~~take~~ [notify the User] upon detection of a potential security violation.
Hierarchical to:	No other components.
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [*not specified*] level of audit; and c) [Other auditable events: - Enabling and disabling of any of the auditing and alarming mechanisms; - All time changes; - Use of the defined management functions; - Unsuccessful login; - Configure and manage cryptographic keys; and - Successful import of user data (keys) - Self-test results].

FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [other audit relevant information: - SNMP log will contain information about the change of the system or network configuration, the source IP address, the username and the action itself; and - The Security Auditing Alarms will contain information about DWDM transmission errors - The User Activity Log that contains information about user activity on CLI interface].
Hierarchical to: Dependencies:	No other components. FPT_STM.1 Reliable time stamps
FAU_GEN.2	**User identity association**
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_SAA.1	**Potential violation analysis**
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [DWDM transmission errors] known to indicate a potential security violation; b) [None].
Hierarchical to: Dependencies:	No other components. FAU_GEN.1 Audit data generation
FAU_STG_EXT.1	**External Audit Trail Storage**
FAU_STG_EXT.1.1	The TSF shall be able to [*transmit the generated audit data to an external IT entity*] using a trusted channel implementing the [*SNMPv3*] protocol.
Hierarchical to:	No other components.

Dependencies:	FAU_GEN.1 Audit data generation

6.1.2 Cryptographic support (FCS)

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 [Nokia's cryptographic key destruction method] that meets the following: [None].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_COP.1(1)	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [encryption and decryption of data] in accordance with a specified cryptographic algorithm [AES (as specified in FIPS 197) encryption (as specified in SP 800-38D) in GCM/GMAC mode] and cryptographic key sizes [256 binary digits in length] that meet the following: [FIPS 140-2 Level 2] and [GdMC].
Application note:	This requirement is provided by the 11QPEN4 or the S13X100E card. The certificate for the cryptographic algorithm used on 11QPEN4 is #tbd (FIPS 197), the S13X100E algorithm certificate is #3844 (FIPS 140-2).
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1(2)	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [software update cryptographic signature verification] in accordance with [SHA512 and RSA Digital Signature Algorithm] and cryptographic key sizes [4096 bits] that meet the following: [- FIPS 180-4 (Secure Hash Standard, SHS) - FIPS 186-4 (Digital Signature Standard)].
Application note:	This requirement is for software updates.

	The correctness of the SHA512 and RSA Digital Signature Algorithm cryptographic implementation regarding FIPS standards is not covered by this evaluation and the algorithms have not yet been FIPS certified. It is covered by vendor assertion.
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1(3)	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [encryption and decryption of management interfaces] in accordance with [SNMP IETF RFC 3411, 3412, 3413, 3414, 3826, HTTPS IETF RFC 2818 and SSH IETF RFC 4251] and cryptographic key sizes [160, 256 bits] that meet the following: [- FIPS 180-4 (Secure Hash Standard, SHS) - FIPS 186-4 (Digital Signature Standard)].
Application note:	This requirement is for management interface security. The correctness of the SSH, HTTPS and SNMPv3 cryptographic implementation regarding FIPS standards is not covered by this evaluation and the algorithms have not yet been FIPS certified. It is covered by vendor assertion.
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

6.1.3 User Data Protection (FDP)

The **Access Control Policy** uses the following definitions:

The subjects are

- a user or process attempting to perform configuration and advanced equipment and service management functions.

The objects are

- MIBs which store the TOE Secondary Assets outlined in Table 3.2: TOE Secondary Assets.

The operations that can be performed with the MIB objects are

- read-view (reading an object)
- write-view (writing an object)
- notify-view (sending objects in a notification)

FDP_ACC.1	**Subset access control**
FDP_ACC.1.1	The TSF shall enforce the [Access Control Policy] on [• Subjects: Users or processes attempting to perform management functions using an SNMP MIB • Objects: MIBs • Operations: read-view, write-view, notify-view].
Hierarchical to: Dependencies:	No other components. FDP_ACF.1 Security attribute based access control
FDP_ACF.1	**Security attribute based access control**
FDP_ACF.1.1	The TSF shall enforce the [Access Control Policy] to objects based on the following: [Subject Security Attributes: Role(s) assigned Object Security attributes: role / access rights (read-view, write-view, notify-view)].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [- the user's role must be assigned the requested access right in the object's set of security attributes].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [- None].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [- None].
Hierarchical to: Dependencies:	No other components. FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ITC.1	**Import of user data without security attributes**
FDP_ITC.1.1	The TSF shall enforce the [Access Control Policy] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [no additional rules].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

6.1.4 Identification and Authentication (FIA)

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.
Hierarchical to:	FIA_UAU.1 Timing of authentication.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UID.2	**User identification before any action**
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UID.1 Timing of identification.
Dependencies:	No dependencies.
FIA_AFL.1	**Authentication failure handling**
FIA_AFL.1.1	The TSF shall detect when [*an Administrator configurable positive integer within **[0 and 15]***] unsuccessful authentication attempts occur related to [the user authentication to the CLI].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall: [- Send an alert message (FAU_STG_EXT.1) - Lock the account, until an Administrator role unlocks it].
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication.
FTA_SSL.3	**TSF-initiated termination**

FTA_SSL.3.1	The TSF shall terminate an interactive session after a [an Administrator configurable positive integer within 1 and 999 (15 minutes by default)].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4	**User-initiated termination**
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1	**TOE access banner**
FTA_TAB.1.1	Before establishing a user session, the TSF shall display **a security specific** advisory **notice and consent** warning message regarding unauthorized use of the TOE.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.5 Security Management (FMT)

FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [- Software update - Management of user logoff. - Management of user accounts. - Management of security and privilege information. - Management of encryption state and cryptographic functions. - Management of system-wide tests. - Management of time stamps. - Management of KMT server connection information - Management of authentication failure lockout - Management of session inactivity timeout - Set minimum password length - Management of audit data - Defining the external IT entity to which audit data is transferred.].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMR.1	**Security roles**

FMT_SMR.1.1	The TSF shall maintain the roles [Crypto Officer, and Administrator].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

6.1.6 Protection of the TSF (FPT)

FPT_STM.1	**Reliable time stamps**
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TST.1	**TSF testing**
FPT_TST.1.1	The TSF shall run a suite of self tests during [***initial start-up***] to demonstrate the correct operation of [***cryptographic functions***].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of [***TSF configuration data***].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of [***TSF software part***].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TUD_EXT.1	**Trusted Update**
FPT_TUD_EXT.1.1	The TSF shall provide **Crypto Officer,** ~~Security~~ Administrator**, NMS and KMT** the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide ~~Security~~ Administrator **and NMS** the ability ~~manually~~ to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall provide a means to verify firmware/software updates to the TOE using a [*digital signature mechanism*] prior to installing those updates.
Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic operation

FPT_RPL.1	**Replay detection**
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [Layer 1 Transport Protocol Encryption].
FPT_RPL.1.2	The TSF shall perform [squelch transmission] when replay is detected.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.2 Security Assurance Requirements

The security target claims an EAL3 security assurance level augmented with AVA_VAN.3 and ALC_FLR.3.

Class	Component
Development	**ADV_ARC.1** Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Guidance Documents	**AGD_OPE.1** Operational user guidance
	AGD_PRE.1 Preparative procedures
Lifecycle Support	**ALC_CMC.3** Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_TAT.1 Well-defined development tools
	ALC_LCD.1 Developer defined lifecycle model
Security Target	**ASE_CCL.1** Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Tests	**ATE_COV.2** Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment	**AVA_VAN.3** Vulnerability analysis

Table 6.1: Security Assurance Components

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

	O_ACCESS	O_ALARM	O_AUDIT	O_CRYPTO_CONFORMITY	O_DATA_CONFIDENTIALITY	O_MANAGEMENT	O_TIME_BASE	O_SW_UPDATE	O_KEY_MANAGEMENT	O_ROLES	O_I&A	O_DISPLAY_BANNER	O_SELF_TESTING	O_RESIDUAL_INFO_CLEARING
FAU_ARP.1 Security alarms		X												
FAU_GEN.1 Audit data generation		X	X											
FAU_GEN.2 User identity association			X											
FAU_SAA.1 Potential violation analysis		X												
FAU_STG_EXT.1 External Audit Trail Storage			X											
FCS_CKM.4 Cryptographic key destruction					X									X
FCS_COP.1(1) Cryptographic operation				X	X									
FCS_COP.1(2) Cryptographic operation				X				X						
FCS_COP.1(3) Cryptographic operation				X		X								
FDP_ACC.1 Subset access control					X	X			X					
FDP_ACF.1 Security attribute based access control					X	X			X		X			
FDP_ITC.1 Import of user data without security attributes					X									
FIA_UAU.2 User authentication before any action	X		X			X			X		X			
FIA_UID.2 User identification before any action	X		X			X			X	X	X			
FIA_AFL.1 Authentication failure handling											X			
FTA_SSL.3 TSF-initiated termination											X			
FTA_SSL.4 User-initiated termination											X			
FTA_TAB.1 TOE access banner												X		
FMT_SMF.1 Specification of Management Functions					X	X			X	X	X			
FMT_SMR.1 Security roles					X	X			X	X	X			
FPT_STM.1 Reliable time stamps		X	X				X							
FPT_TST.1 TSF testing													X	
FPT_TUD_EXT.1 Trusted Update								X						
FPT_RPL.1 Replay detection				X										

Table 6.2: Security Requirements to Security Objectives Mapping

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the following table.

Security Objective(s)	Rationale
O_ACCESS	O_ACCESS requires the TOE to protected against non-authorized logical access and provide mechanisms for authenticating users before granting access to the functions. The security functional requirements FIA_UAU.2 and FIA_UID.2 require the TOE to implement a user identification and authentication before allowing any other TSF-mediated actions on behalf of that user as demanded by O_ACCESS. Therefore, FIA_UAU.2 and FIA_UID.2 are suitable to meet the security objective.
O_ALARM	The security objective is covered as follows. The security functional requirement FAU_ARP.1 requires that the user will be notified upon detection of a potential security violation,while FAU_SAA.1 assigns the monitoring rules. FAU_GEN.1 defines the generation of audit records more precisely and FPT_STM.1 provides these records with reliable time stamps.
O_AUDIT	O_AUDIT requires the TOE to provide logs which are write-protected and only accessible to an Administrator. The SFR FAU_GEN.2 requires for audit events resulting from actions of identified users an association of each auditable event with the identity of the user that caused the event. Therefore, the audit records must reliably be generated as defined by FAU_GEN.1 and FPT_STM.1. The users must be identified and authenticated as defined by FIA_UID.2 and FIA_UAU.2 to bind actions to a user.The SFR FAU_STG_EXT.1 requires audit records be sent to an external IT entity for storage and viewing. All SFRs mentioned exactly require to implement SNMP Logs, security event logs and user activity log as defined by O_AUDIT.
O_CRYPTO_CONFORMITY	The security requirement FCS_COP.1(1), FCS_COP.1(2) and FCS_COP.1(3) define the cryptographic operations in more detail. The cryptograhic algorithms meet the FIPS 140-2 L2 standard and ANSSI RGS Annex B1. Replay-attacks are handled according to FPT_RPL.1.

Security Objective(s)	Rationale
O_DATA_CONFIDENTIALITY	O_DATA_CONFIDENTIALITY requires the TOE to protect the confidentiality of D_DATA. This is fulfilled by the security functional requirements FCS_COP.1 and its dependent SFRs. FCS_COP.1 depends on FDP_ITC.1 and FCS_CKM.4. Whereas, FDP_ITC.1 describes the import of user data without security attributes and is related to the Security Function Policy (SFP) “Access Control Policy”. The keys are stored in volatile memory and the key data is lost upon power-off or the extraction of the cryptographic module from the TOE. For key replacement, the encryption module provides a procedural method controlled via the management interface that includes overwriting the volatile key in RAM at least once. In addition, the dependend security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1 and FMT_SMF.1 are needed. They are also related to the SFP “Access Contorl Policy”. FDP_ACC.1 and FDP_ACF.1 enforce this SFP on subjects, objects, operations and attributes. The security roles needed and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, FMT_SMF.1 specifies management functions for cryptography.
O_KEY_MANAGEMENT	O_KEY_MANAGEMENT requires the TOE to provide authenticated and authorized users management and configuration mechanisms for D_CRYPTO_KEYS, D_CONFIG_KEYS, the equipment and its cryptographic functions. The security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_SMF.1, FIA_UAU.2 and FIA_UID.2 and the related SFP “Access Control” exactly require to implement this kind of management and configuration mechanisms. FDP_ACC.1 and FDP_ACF.1 enforce the Access Control Policy on subjects, objects, operations and attributes. The security roles and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, the users authentication is required within FIA_UAU.2. FMT_SMF.1 specifies different management functions. For example, the management of advanced equipment and service management functions is specified here. Therefore, the mentioned SFRs in combination with the related SFP “Access Control Policy” provide authenticated and authorized users management and configuration mechanisms for the defined objects. In particular, these objects comprise D_CRYPTO_KEYS, D_CONFIG_KEYS, the equipment and its cryptographic functions as demanded by O_KEY_MANAGEMENT and O_MANAGEMENT.

Security Objective(s)	Rationale
O_MANAGEMENT	O_MANAGEMENT requires the TOE to provide authenticated and authorized users management and configuration mechanisms for D_AUDIT, D_CONFIG_KEYS, D_TIME_BASE and D_CONFIG_MANAGEMENT, the equipment and its cryptographic functions. The security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_SMF.1, FIA_UAU.2 and FIA_UID.2 and the related SFP “Access Control” exactly require to implement this kind of management and configuration mechanisms. FDP_ACC.1 and FDP_ACF.1 enforce the Access Control Policy on subjects, objects, operations and attributes. The security roles and the identification of users are defined within FMT_SMR.1 and FIA_UID.2. Additionally, the users authentication is required within FIA_UAU.2. FMT_SMF.1 specifies different management functions. For example, the management of advanced equipment and service management functions is specified here. Therefore, the mentioned SFRs in combination with the related SFP “Access Control Policy” provide authenticated and authorized users management and configuration mechanisms for the defined objects. In particular, these objects comprise D_AUDIT, D_CONFIG_KEYS, D_TIME_BASE and D_CONFIG_MANAGEMENT, the equipment and its cryptographic functions as demanded by O _MANAGEMENT. FCS_COP.1(3) specifies the cryptographic algorithms to be used for this operation.
O_TIME_BASE	This objective is covered by the requirement FPT_STM.1.
O_SW_UPDATE	The security objective is covered by FPT_TUD_EXT.1 which requires software integrity and authentication checking. FCS_COP.1(2) specifies the cryptographic algorithms to be used for this operation.
O_ROLES	The security functional requirement FMT_SMR.1 and FIA_UID.2 require the maintenance of the Administrator and Crypto Officer role as well as the identification before any action of these users. FMT_SMF.1 specifies role management functions. This is exactly required by O_ROLES and therefore O_ROLES is fulfilled.

Security Objective(s)	Rationale
O_I&A	The security objective O_I&A is covered as follows. The security functional requirement FIA_UID.2 and FIA_UAU.2 require the identification and authentication of a user before any action of these users. FMT_SMR.1 requires the TOE to manage user roles, while FMT_SMF.1 specifies role management functions. FIA_AFL.1 specifies the behavior of the TOE in case of user authentication failure. FTA_SSL.3 and FTA_SSL.4 requires TSF and User-initiated session termination. For remote management, FDP_ACF.1 requires the device to be identified before granting it access to management functionalities. FIA_AFL.1 requires the TOE to detect when a configurable number of authentication attempts is met.
O_DISPLAY_BANNER	The security objective is covered by FTA_TAB.1 which requires the TOE to display a banner to the user regarding unauthorized use of the TOE.
O_SELF_TESTING	The security objective is covered by FPT_TST.1.
O_RESIDUAL_INFO_CLEARING	The security objective is covered by FCS_CKM.4 which requires destruction of D_CRYPTO_KEYS after use.

Table 6.3: Security Objectives to Security Requirements Rationale

6.3.2 Rationale for SFR Dependencies

SFR	Dependencies	Fulfilled by SFRs in this ST
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	--
FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 See discussion below.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 See discussion below
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	--	--
FIA_AFL.1	FIA_UAU.1	FIA_UID.2
FTA_SSL.3	--	--
FTA_SSL.4	--	--
FTA_TAB.1	--	--
FMT_SMF.1	--	--
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	--	--
FPT_TST.1	--	--
FPT_TUD_EXT.1	FCS_COP.1	FCS_COP.1(2)
FPT_PRL.1	--	--

Table 6.4: Dependencies for Security Functional Requirements

The dependencies of FDP_ACF.1 and FDP_ITC.1 address the management of security attributes and their initialisation. The dependency FMT_MSA.3 is not included within this Security Target, since security attributes are only implicitely contained within the definition of subjects. There do not exist any explicitly defined security attributes.

The dependencies of FCP_COP.1(2) address the cryptographic keys used to verify the integrity and authentication:

- The dependency “[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]” is replaced by the software update itself (FPT_TUD_EXT.1): cryptographic keys are renewed during this operation.
- The dependency “FCS_CKM.4” is unsatisfied otherwise no more software update could be performed after a key erasing.

6.3.3 Security Assurance Requirements Rationale

The TOE evaluation is performed in regards to CC EAL3 security assurance level augmented with ALC_FLR.3 and AVA_VAN.3.

7. TOE Summary Specification

The TOE provides the following security services:

- Layer 1 transport protocol encryption
- Secure Management
- Self-testing
- User Authentication, Authorization and Audit Logs
- Potential Intrusion Alarms

7.1 Layer 1 transport protocol encryption

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Cryptographic Support.

SFR	Rationale
FCS_COP.1(1)	The TOE has four instances of one implementation of AES GCM 256 bits: The 11QPEN4 encryption card contains a single FPGA which has four separate AES instances that will each encrypt 10G of traffic on to each of the four 10G optical fiber interfaces. This implementation [will be] has been awarded algorithm certificate number A2539 by the CAVP. The TOE has one instance of one implementation of AES CTR + GMAC 256 bits: The S13X100E encryption card contains an single ASIC which will encrypt the traffic on the 100G optical fiber interface. This implementation has been awarded algorithm certificate number #3844 by the CAVP.
FCS_CKM.4	The TOE implements a destruction methods of cryptographic keys when they are no more used.
FPT_RPL.1.1	The TOEs implementations of AES GCM and AES GMAC implements a replay detection of the counter for each instance.
FPT_RPL.1.2	If the TOE detects a replay of the counter in an instance then the transmission of this instance is squelched.

Table 7.1: Rationale For Cryptographic Support

7.2 Secure Management

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Secure Management.

SFR(s)	Rationale
FDP_ACC.1 **FDP_ACF.1** **FDP_ITC.1**	The access to management and encryption functions is only possible after successful user authentication and authorization as an Administrator. The 11QPEN4 Session Encryption Key is an AES-256 key that is imported across an encrypted SNMPv3 link from the KMT. The S13X100E Session Encryption Key is an AES-256 key that is imported across an encrypted SNMPv3 link from the KMT.
FMT_SMF.1	An important and critical part of the TOE configuration is the initial configuration, during which the Secure Management interfaces (with NMS and KMT), authentication parameters and other security settings are configured. The initialization of the keys for the Secure Management interface SNMP is done out-of-band and using pre-shared keys. The initialization of the usernames and passwords for the Secure Management interface using SSH and HTTPS is done out-of-band and using pre-shared passwords. The TOE performs management functions of initialization; activation and deactivation on fault detection during system startup and provides logging of successful selftest completions and alarms and logs for unsuccessful selftests.
FMT_SMR.1	The TOE provides different user roles for different operators (Administrator, Crypto Officer). Refer to Table *1.5:* User Roles for a list of the functions that can be performed by each role.
FCS_COP.1(2)	The TOE checks the integrity and authentication of software updates after software download and prior installing it. This verification is based on SHA-512 and RSA 4096 bits operations performed on the full software RPM.
FCS_COP.1(3)	The TOE provides confidentiality and integrity at the SSH, HTTPS and SNMPv3 based management interfaces.
FPT_TUD_EXT.1	The TOE offers to the Crypto Officer, the Administrator, the NMS and the KMT the capability to query the current software version It provides also a software update funtionality to Administrator and the NMS, that checks the integrity and authentication of software updates after software download and prior installing it.

Table 7.2: Rationale for Secure Management

7.3 Self-testing

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Self-test.

SFR(s)	Rationale
FPT_TST.1	A start-up, the TOE performs selt-tests on the software and on the cryptographic functions. After software integrity self test, crypto self test are performed on : - AES GMAC or AES GCM (depending on HW) - SHA - SHA with RSA signature Self-test results are logged in the audit record. the TOE provides also the Administrator and the Crypto Officer with the capability to request integrity testing on configuration data and on the software.

7.4 User Authentication, Authorization and Audit Logs

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for the SNMP log, security event log and user activity log.

SFR(s)	Rationale
FAU_GEN.1 **FAU_GEN.2**	The TOE will record security relevant user activities in the SNMP log which is in a user-readable format. Each entry in the SNMP log will contain the time and date of the action, the source IP address, the user name and the action itself. The TOE also records the important security relevant events not resulting directly from an SNMP request in the security event log. The TOE will record the triggering of the DWDM transmission alarm in the Security Auditing Alarms. Each entry will contain the date and time of the alarm, the alarm source (shelf/slot/port), the card type, the category of the component, the severity (Critical, Major, Minor, Warning), description of the alarm, alarm type, indicator if a service has been affected, and additional information/data about the alarm.
FAU_STG_EXT.1	The TOE will transmit audit records sent to the SNMP log and security event log to an external IT entity using SNMP v3. The audit records are usually sent to an NMS or external log server.
FIA_UAU.2 **FIA_UID.2** **FIA_AFL.1** **FTA_TAB.1** **FTA_SSL.3** **FTA_SSL.4**	An individual must be successfully authenticated as either an Administrator, or Crypto Officer before the TOE will provide access to any of it's services. In case of too much unsuccessful authentication attempts (the threshold is configurable), the user account is locked until an Administrator role unlocks it. When opening a user session, the TOE displays a security specific advisory notice message regarding unauthorised use of the TOE. The user session is terminated after 3 minutes of user inactivity or at user request.
FPT_STM.1	The TOE maintains a reliable time to be used in time stamps for audit records.

Table 7.3: Rationale for User Authentication, Authorization and Audit Logs

7.5 Potential Intrusion Alarms

The following table provides the rationale and evidence for how the TOE meets each of the SFRs for Potential Intrusion Alarms.

SFR(s)	Rationale

FAU_ARP.1
FAU_SAA.1
	The TOE implements the following for the detection of a potential intrusion or an attempt to hide another type of attack:
	• DWDM transmission alarm
	  ○ Will detect potential attempts to gain physical access to the optical fiber.
	  ○ A sample scenario that would trigger this alarm, is a Threat Agent disturbing the optical transmission in order to hide an ongoing attack against the fiber or the Neighboring Equipment.

Table 7.4: Rationale for Potential Intrusion Alarms

END OF DOCUMENT

