# Security Target

# Alcatel-Lucent

# 1830 Photonic Service Switch (PSS) R7.0

Version 0.14

Date: 12 June 2015

# Table of Contents

# List of Tables

# List of Figures

# 1. Security Target Introduction

This Security Target is for the Common Criteria evaluation of the Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0 for DWDM (Dense Wavelength Division Multiplexing) networks based on Alcatel-Lucent's 1830 Photonic Service Switch (PSS) and the 11QPEN4 (Quad Port Encryption) Transponder.

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 1830 PSS is a scalable DWDM platform that supports aggregation for Ethernet, Fibre Channel (FC) and other protocols. The 1830 PSS provided the first commercially available support for 100G next generation coherent technology building on the Zero-Touch Photonics approach, which enables easier operations for reduced costs and accelerated provisioning of wavelength services. In contrast to traditional DWDM technologies, the Zero Touch Photonic eliminates the need for frequent on-site interventions and provides a network that is more flexible to design and install, easier to operate, manage, and monitor, where wavelength services can be deployed faster and reconfigured according to more dynamic traffic demands. These are important capabilities for datacenter customers, who are more focused than traditional operators on the application layer and Service Level agreements (SLA) than on the network itself. As datacenters continue to evolve, high speed DWDM interconnection technology will be essential not only for data mirroring but also for other types of applications. Instead of just point-to-point high capacity links, more complex topologies with bandwidth allocation on demand will be needed for scenarios requiring the transparent and hitless migration of large virtual machines and provisioning of cloud services over geographically distributed storage points or hosts, while maintaining high performance and security across datacenters.

Data confidentiality is a key security requirement for datacenters, in particular for customers operating under certain legal frameworks and in specific business sectors. It is difficult to guarantee confidentiality for a leased fiber traversing the many kilometers between secured datacenter facilities or over a shared DWDM or switched network. Layer 1 encryption provides end-to-end protection against loss of confidentiality along the fiber. Encryption at this layer also provides independence in the selection of protocols or applications used at higher layers, as well as lower encryption latency than possible with other technologies. 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 Advanced Encryption Standard (AES) 256 encryption 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 module also supports diverse types of data interfaces used by service providers and increasingly used by carriers like 8G/10G fibre channel, 10G Ethernet interface (10GE) and Optical Transport Unit 2 (OTU2). The solution also provides a capability for guarding against an intruder tapping power from an optical fiber. A hacker who may gain physical access to a fiber could bend it so that some light leaks out of the fiber. The intruder could then use a commercial photo detector to attempt to recover the data carried in the optical signal.

For the complex security scenarios necessary for government organizations, healthcare and financial institutions, the Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0 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 Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0 |
| Version: | 0.14 |
| Publication Date: | 12 June 2015 |
| Author: | Alcatel-Lucent Optical Division |

## 1.2 TOE Identification

| | |
|---|---|
| Name: | 1830 Photonic Service Switch (PSS) |
| Version: | R7.0, build number 16.18-0 |
| Sponsor: | Alcatel-Lucent |
| Developer: | Alcatel-Lucent |
| Keywords: | DWDM, datacenter, interconnection, encryption |

## 1.3 Target of Evaluation (TOE) Overview

Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0 is based on the encryption card 11QPEN4 installed on an 1830 PSS shelf with an Equipment Controller (EC). The TOE consists of both hardware and software as shown in Figure 1 and Figure 2 and identified in shaded areas.

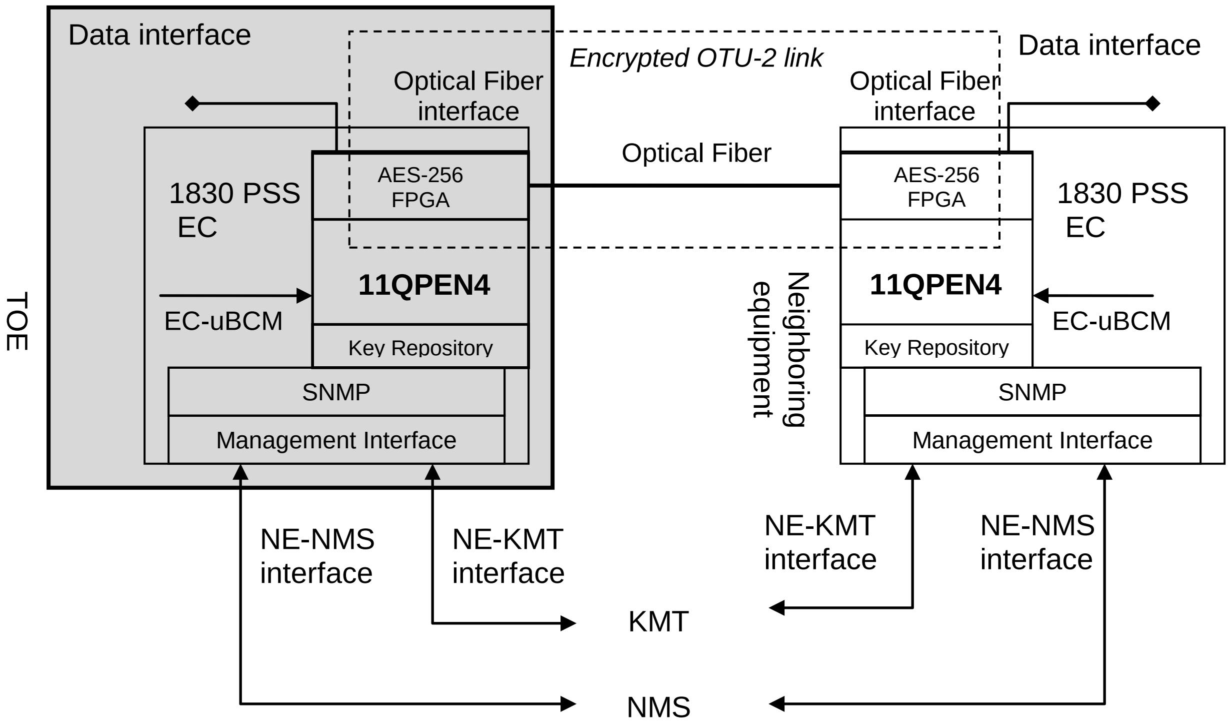

*Figure 1 – 1830 Photonic Service Switch (PSS) R7.0*

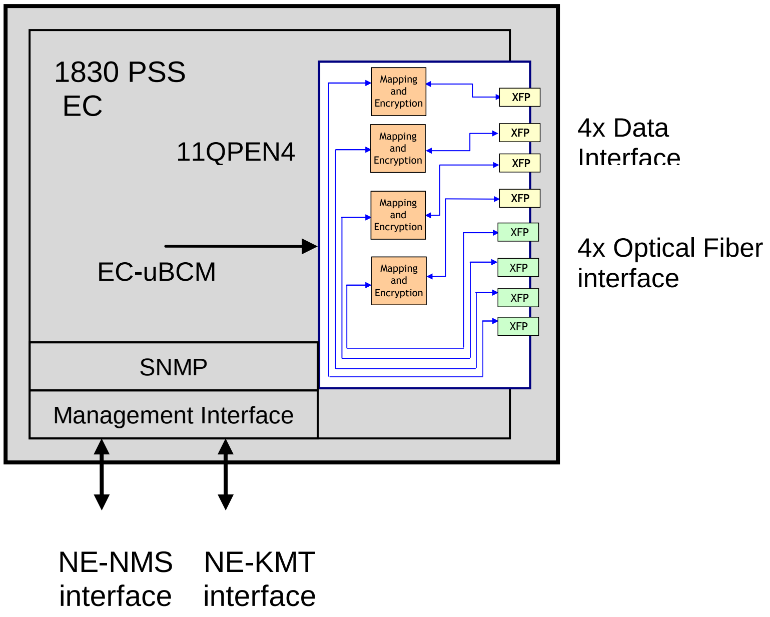

*Figure 2 – 1830 Photonic Service Switch (PSS) R7.0 - Detail with 11QPEN4 schematics and no neighboring equipment*

The interfaces covered by the TOE are:

a) The data interfaces to connect external client equipment (located inside a trusted or internal network);

b) The Optical Fiber interfaces (OTU-2) to connect the TOE to similar neighboring equipment (systems located on a trusted or internal network) and the fibers between the systems extend through an untrusted or public network; and

c) The Management Interface to configure and manage the TOE via external equipment using SNMP:

   The Management Interface can be used to connect the TOE to an external Network Management System (NMS) and a Key Management Tool (KMT), which are distinct non-TOE products intended to facilitate the configuration and management of the equipment and its cryptographic functions.

The security features covered by the TOE are:

a) Cryptographic Support;

b) Secure Management;

c) User Authentication, Authorization and Audit Logs; and

d) Potential Intrusion Alarms.

### 1.3.1 Operational Environment

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 a second 1830 PSS connected via the optical fiber to the TOE in a remote site as shown in Figure 1. | ITU-T G.709 and Advanced Encryption Standard AES-256 in CTR mode |
| Third Party Browser | An Internet Explorer browser with TLS/SSL support is used for initial configuration of the TOE and troubleshooting via the Management Interface and the Web-UI component. The interface will be disabled as part of the TOE in FIPS Mode.<br>Only the FIPS Mode is covered by this certification. | TLS/SSL IETF RFC 5246 |

| | | |
|---|---|---|
| Network Management System (NMS) | The NMS is an external system that can be used to administer and operate the TOE via the Management Interface.<br>The NMS uses SNMPv3 to communicate with the TOE. | SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 |
| Key Management Tool (KMT) | The KMT is an external web-based application that can be used to manage the cryptographic functions of the TOE via the Management Interface.<br>The KMT uses SNMPv3 to communicate with the TOE. | SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 |
| SFTP client | A SFTP client can be enabled to upload software, perform DB backups from the NMS and collect SNMP and audit logs. Guidance instructs administrators to not perform software upgrades or back up the database when in FIPS mode.<br>The SFTP client will not be covered by this certification. | SSH IETF RFC 4251 |
| SSH client | A SSH client can be used only for initial configuration and troubleshooting via the Command Line Interface (CLI), while not in FIPS Mode. Then the SSH-CLI server will be disabled as part of the TOE in FIPS Mode. Only the FIPS Mode is covered by this certification. | SSH IETF RFC 4251 |

***Table 1.1: Non-TOE Comonents***

## 1.4 TOE Description

### 1.4.1 Scope of Evaluation

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

#### 1.4.1.1 Physical Scope

The following TOE components are covered by the physical scope. All three of the PSS32/PSS16/PSS4 platforms are hardware modules with multi-chip standalone embodiments.

| TOE Component | Subcomponent | Description |
|---|---|---|
| 1830 PSS-32 | EC PSS-16/PSS-32 | EC - Equipment Controller - 16G flashcard |
| | 11QPEN4<br>(16 maximum per 1830 PSS-32 shelf, slots 2–17) | Encryption card - SAN ENC Kit (11QPEN4 + SWL for 1-port)<br>10GBASE-SR XFP - Client XFP short reach, 850nm, 10 GE<br>X8FCLC-L XFP - XFP I-64.1/8.5GFC IT (8G FC XFP SM)<br>X8FCSN-I XFP - 8G FC XFPMM<br>XI-64.1 XFP - 10G FC - OTM-0.2/e/f (P1I1-2D1), SMF 1310nm 10km<br>XL-64TU XFP - DWDM Tunable CT (50GHz 10G XFP)<br>eVOA_P SFP - Fast electronic Variable Optical Attenuator (Fast eVOA) |
| | PSS-32 Main Shelf kit (includes high-capacity fan) | Main Shelf |
| | PSS-32 User Panel | User Panel |
| | Security Label Kit | 30 tamper-evident labels |
| | Power supply | PF (−48V DC) PSS-32 |
| | Filler plates | FSBNK: Full-slot blank<br>HSBNK: Half-slot blank |
| | High-Capacity Fan | High-Capacity Fan |
| 1830 PSS-16 | EC PSS-16/PSS-32 | EC - Equipment Controller - 16G flashcard |
| | 11QPEN4<br>(3 maximum per 1830 PSS-16 shelf, slots 7–9) | Encryption card - SAN ENC Kit (11QPEN4 + SWL for 1-port)<br>10GBASE-SR XFP - Client XFP short reach, 850nm, 10 GE<br>X8FCLC-L XFP - XFP I-64.1/8.5GFC IT (8G FC XFP SM)<br>X8FCSN-I XFP - 8G FC XFP MM<br>XI-64.1 XFP - 10G FC - OTM-0.2/e/f |

| TOE Component | Subcomponent | Description |
|---|---|---|
| | | (P1I1-2D1), SMF 1310nm 10km<br>XL-64TU XFP - DWDM Tunable CT (50GHz 10G XFP)<br>eVOA_P SFP - Fast electronic Variable Optical Attenuator (Fast eVOA) |
| | ANSI Bay Frame Kit | Frame Kit |
| | PSS-16 Main Shelf kit | Main Shelf |
| | PSS-16 User Panel | User Panel |
| | Security Label Kit | 30 tamper-evident labels |
| | Power supply | PF (−48V DC) PSS-16 |
| | Filler plates | FSBNK: Full-slot blank<br>HSBNK: Half-slot blank |
| | PSS16 Fan Tray | Fan Tray |
| 1830 PSS-4 | EC PSS-4 | ED 4 Equipment Controller |
| | 11QPEN4 (1 maximum per 1830 PSS-4 shelf, slot 7) | Encryption card -SAN ENC Kit (11QPEN4 + SWL for 1-port)<br>10GBASE-SR XFP - Client XFP short reach, 850nm, 10 GE<br>X8FCLC-L XFP - XFP I-64.1/8.5GFC IT (8G FC XFP SM)<br>X8FCSN-I XFP - 8G FC XFPMM<br>XI-64.1 XFP - 10G FC - OTM-0.2/e/f (P1I1-2D1), SMF 1310nm 10km<br>XL-64TU XFP - DWDM Tunable CT (50GHz 10G XFP)<br>eVOA_P SFP - Fast electronic Variable Optical Attenuator (Fast eVOA) |
| | ANSI Bay Frame Kit | Frame Kit |
| | PSS-4 Shelf | ED 4 Shelf (Shelf, BP, Shelf ID, Dust Filter) |
| | Fan | ED 4 Fan Unit Hardened |
| | Security Label Kit | 30 tamper-evident labels |
| | Power Filter | ED 4 Power Filter (−48 V DC) with WT-Hardened |

| TOE Component | Subcomponent | Description |
|---|---|---|
| | | ED 4 Power Filter (−48 V DC) with WT EM-Hardened<br>ED 4 Power Filter (AC) with WT-Hardened<br>ED 4 Power Filter (+24 V DC) with WT- Hardened |
| | Filler plates | E4FSFB: ED 4 Static Filter Blank (full slot)<br>FSBNK: Full-slot blank |
| | FIPS Kit | PSS-4 FIPS Kit (Bracket and Air Baffle) |

***Table 1.2: Physical Scope***

After manufacturing and delivery to customer premises, the TOE is verified, initialized and customized by qualified Alcatel-Lucent 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.

### 1.4.1.2 Guidance Documentation

The TOE includes the following user and administrative guidance:

Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) Release 7.0 User Provisioning Guide

Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) Release 7.0 Installation and System Turn-up Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 User Provisioning Guide

Alcatel-Lucent 1830 Photonic Service Switch 16/32 (1830 PSS-16/PSS-32) Release 7.0 Installation and System Turn-up Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Maintenance and Trouble-Clearing Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Command Line Interface Guide

Alcatel-Lucent 1830 1354 RM-PhM Photonic Manager Release 12.0 EMS Reference Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) Administration Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) User Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) Installation Guide

Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0.0 Federal Information Processing Standards (FIPS) User Guide and Logbook

#### 1.4.1.3 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 certified 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. 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.

### 1.4.2 Summary of Security Features

The TOE comprises the following security features.

#### 1.4.2.1 Cryptographic Support

The cryptographic function of the TOE is implemented by means of the 11QPEN4 card, which is a full height, single-slot standalone card providing OTU-2 line encryption with AES-256. The utilization of AES-256 in CTR mode provides strong encryption for the four separated optical fiber interfaces in each 11QPEN4 pack.

Layer 1 encryption provides 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 than that possible with higher level protocols of the TCP/IP and OSI stacks.

The SNMPv3 management interfaces also provide AES, SHA-1, and HMAC-SHA-96 implementations.

The cryptographic operations implemented by the 11QPEN4 encryption card and SNMPv3 satisfy the FIPS 140-2 Level 2 requirements.

### 1.4.2.2 Secure Management

The TOE provides encrypted interfaces for SNMPv3 management functions accessed via the physical Management Interface. The access to management and encryption functions is only possible after successful user authentication and authorization.

An important part of the TOE configuration is the transformation of the system to FIPS Mode, which enables the Secure Management interfaces (SNMPv3), authentication parameters and other security settings. The initial configuration of the keys for the Management Interface is done offline and using pre-shared keys.

The physical Management Interface provides the following generic components:

| Management Interface Component | Interface Description | TOE's Settings | Applicable Standards |
|---|---|---|---|
| NE-NMS | The NE-NMS interface can be used to connect an external Network Management System (NMS) for administration and operation of the TOE.<br>NOTE: The NMS system is in the operational environment. The | SNMPv3 is configured both as server (commands) and client (notifications) in AuthPriv mode:<br>-Authentication: HMAC-SHA-1-96<br>-Privacy: AES 256 in CFB128 mode of operation<br>The lower layers of the Management Interface are based on Ethernet 100BaseT. | SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 |
| NE-KMT | The NE-KMT interface can be used to connect an external Key Management Tool for cryptographic administration and operation of the TOE.<br>NOTE: The KMT system is in the operational environment. | SNMPv3 is configured both as server (commands) and client (notifications) in AuthPriv mode:<br>-Authentication: HMAC-SHA-1-96<br>-Privacy: AES 256 in CFB128 mode of operation<br>The lower layers of the Management Interface are based on Ethernet 100BaseT. | SNMP IETF RFC 3411, 3412, 3413, 3414 and 3826 |

***Table 1.3: Secure Management Interfaces***

After the transformation to FIPS Mode, and in order to reduce the attack surface of the TOE, other management interfaces available by default and not listed above will be disabled. FIPS Mode also disables 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. Only the FIPS Mode of operation is covered by this evaluation.

The TOE supports different user roles. Roles can be assigned to users during system commissioning and are consistently applied for access via the management interfaces listed in Table 1.3.

| Role | Privileges |
|---|---|
| Administrator | These roles are the administrator of the TOE. This role provides all services that are necessary for initial installation of the module. This user can configure the system and perform provisioning and testing of all IO cards, ports, interfaces, and circuits. The user can also create, delete, and modify user accounts, as well as manage security and cryptographic functions and parameters. This user does not have access to the debug and SW development tools. A summary of what this user can do is:<br>• retrieve security information about users (not password);<br>• 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;<br>• configure IO cards, ports, interfaces and circuits;<br>• run test procedures on any card that does not contribute to system-wide outage;<br>• provision the TOE;<br>• create and manage encryption circuits; and<br>• manage cryptographic parameters and functions. |
| Crypto Officer | This is the administrator for the cryptographic keys. A summary of what this user can do is:<br>• set encryption state and encryption keys;<br>• obtain own user info, |

**Table 1.*4: User Roles***

Other default accounts, used for instance for initial commissioning or service, will be disabled as part of FIPS Mode, i.e. other default accounts are not covered by this evaluation.

### 1.4.2.3 User Authentication, Authorization and Audit Logs

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

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

Security-related auditable events are recorded in the SNMP log or in the security event log. 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.

#### 1.4.2.3.1 SNMP log

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

1.4.2.3.2 Security Event Log

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

### 1.4.2.4 Potential Intrusion Alarms

The TOE provides security notifications for the detection of a potential intrusion or an attempt to hide another type of attack:

- **DWDM Transmission Alarms:** This type of alarms, which are generic to DWDM technology and not explicitly related to security, can be used to detect potential attempts to gain physical access to the optical fiber. A possible scenario is a Threat Agent disturbing the optical transmission in order to hide an ongoing attack against the fiber or the Neighboring Equipment.

## 1.4.3 Logical Functionality and Interfaces Not Included in the TOE

The following are excluded from this certification. These features are disabled in the evaluated configuration:

- Software Download;
- Database backup and restore;
- Third Party Browser, except during initial configuration
    - Web-UI;
    - TLS/SSL support;
- Telnet support;
- SSH support, except during initial configuration;
- RADIUS support;
- NTP server support; and
- Provisioner and Observer roles.

The NMS and/or KMT system in the operational environment provides a user friendly interface for the SNMP interface to the TOE. The administrator can view audit records as they are received by the NMS or KMT system.

SFTP can be used to perform backups of the PSS. The use of SFTP is not covered by this evaluation.

The following features are not disabled in the evaluated configuration, but are excluded from use in the certification:

- Command Line Interface (CLI) via serial port
- WebUI
- NMS role

# 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-2012-09-001, Version 3.1, Revision 4, September 2012 [CCP1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CCP2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CCP3]

as follows:

- CC Part 2 conformant
- CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 [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 2+ augmented with ALC_FLR.2.

# 3. TOE Security Problem Definition

## 3.1 Overview and Definitions

The primary asset that will be protected by the TOE:

| Asset | Definition |
|---|---|
| **D_DATA** | Data in the fiber between the TOE and the neighboring 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.

The secondary assets 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. |
| **D_CONFIG_KEYS** | Symmetric and asymmetric keys used for encryption and decryption of D_MANAGEMENT. |
| **D_CONFIG_MANAGEMENT** | Configuration parameters of the TOE via the management interfaces. |
| **D_AUDIT** | 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. |
| **D_MANAGEMENT** | Management data in the out-of-band channel between the TOE and non-TOE components as defined in Table 1.1. |

***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.

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 provision and switch the Encryption Key.  The Crypto Officer is a privileged user with Crypto Officer rights defined in Table *1*.4. |
| **User:** | The Administrator is a user or process authorized to perform configuration |

| Subject | Description |
|---|---|
| **Administrator** | and advanced equipment and service management functions.<br>The Administrator is a privileged user with Administrative rights, which include user management and cryptographic management as defined in Table *1*.4. |
| **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 financial advantage of D_DATA. |

***Table 3.3: Subjects and External Entities***

## 3.2 Assumptions

The following assumptions apply to the TOE environment.

| Assumption | Description |
|---|---|
| **A_ADMIN** | It is assumed that trusted and well trained users will administer the TOE. |
| **A_AUDIT** | It is assumed that alarms are monitored and SNMP Logs and security event logs are regularly examined by the administrator and corrective actions are taken upon potential incident detection according to Alcatel-Lucent recommendations for managing the TOE. |
| **A_CONFIGURATION** | It is assumed that the TOE is configured following Alcatel-Lucent recommendations in order to properly protect the primary and secondary assets of the TOE.<br>It is assumed that Neighboring Equipment and non-TOE components, as defined in Table 1.1, are configured following the vendor security recommendations. |
| **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_PROTECTION** | It is assumed that the TOE is protected as follows:<br>a) The TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access to the TOE.<br>b) Non-TOE management assets, secondary assets and the Neighboring Equipment have at least the same level of physical and logical protection as the TOE.<br>c) User data intended for transmission via the TOE including D_DATA and the defined secondary assets are protected. It is also assumed that data originating from the TOE is handled securely. |

*Table 3.4: Assumptions*

### 3.2.1 Threats Averted by the TOE

According to [ITU_1], the following general threats apply to a data communication system:

a) Destruction of information and/or other resources;
b) Corruption or modification of information;
c) Theft, removal or loss of information and/or other resources;
d) Disclosure of information; and
e) Interruption of services.

These threats can be classified as accidental or intentional and may be active or passive. An active attack is for instance a Denial of Service (DoS) attack, while passive attacks are such as the modification or deletion of authentication information (e.g., user identifications and passwords, administrator identifications and passwords). An accidental attack is for instance a non-intentional modification leading to interruption of services (e.g., critical parameter change).

Some of these threats will be covered by the product itself, while others by the environment.

The following table definition describes the threats to be averted by the TOE.

| Threat | Description |
|---|---|
| **T_DATA_DISCLOSURE** | This category covers the threats by which a Threat Agent illicitly accesses the optical fiber using a fiber-taping device in order to compromise D_DATA with the objective to perform a disclosure of information. |
| **T_CONFIG_EXTRACTION** | This category covers the threats by which a Threat Agent illicitly accesses the TOE through the Management Interface or another interface in order to covertly read resources like D_CRYPTO_KEYS, D_CONFIG_KEYS, D_AUDIT, D_CONFIG_MANAGEMENT and D_MANAGEMENT, which can be used for subsequent attacks against D_DATA. |
| **T_CONFIG_MODIFICATION** | This category covers the threats by which a Threat Agent illicitly accesses the TOE through the Management Interface or another interface in order to interrupt services; or modify, corrupt or destruct resources like D_CONFIG_KEYS, D_CRYPTO_KEYS, D_MANAGEMENT, D_CONFIG_MANAGEMENT or D_AUDIT. |

*Table 3.5: Threats Adverted by the TOE*

The equipment architecture guarantees that attacks against management plane objects like D_CRYPTO_KEYS, D_CONFIG_KEYS, D_CONFIG_MANAGEMENT, D_MANAGEMENT and D_AUDIT are not possible via the data plane (i.e. optical fiber interface and data interface). According to Common Criteria this protection aspect is evaluated within the scope of the class ADV_ARC. This protection is achieved by means of a strict separation of user and management planes as defined in [ITU_2]. The control plane is disabled as part of the Secure Mode configuration and cannot be used as an extraction channel for TOE configuration parameters.

The logical protection of the equipment itself against penetration attacks is subject to evaluation within the class ADV_ARC of CC.

To operate in FIPS Approved mode tamper evident seals shall be installed, replaced and inspected as indicated in the equipment documentation, see Table 1.2: Physical Scope.

## 3.3 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 | Description |
|---|---|
| **OSP_ACCESS** | The TOE shall provide logical access control mechanisms. 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 authenticated and authorized users 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. |

***Table 3.6: OSP Applicable to the TOE***

General management functions can be implemented via non-TOE components, which should include facilities for fault, configuration, accounting, performance, security management as defined in [ITU_3]. Cryptographic management functions can be implemented via non-TOE components, which should facilitate the management of the key lifecycle.

# 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.

| Objective | Description |
|---|---|
| **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:<br>a) DWDM Transmission Errors |
| **O_AUDIT** | The TOE shall record security relevant events, such asTOE configuration changes. The TOE must transmit audit data to an external trusted entity for storage and viewing. |
| **O_CRYPTO_CONFORMITY** | The TOE shall provide D_DATA encryption and decryption which will conform to the FIPS 140-2 Level 2 requirements. |
| **O_DATA_CONFIDENTIALITY** | The TOE shall protect the confidentiality of D_DATA. |
| **O_KEY_MANAGEMENT** | The TOE shall provide mechanisms and procedures 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_MANAGEMENT_CONFIDENTIALITY** | The TOE shall provide mechanisms to protect the confidentiality of D_CRYPTO_KEYS, D_CONFIG_KEYS, D_AUDIT, D_CONFIG_MANAGEMENT and D_MANAGEMENT. |
| **O_MANAGEMENT_PROTECTION** | The TOE shall provide mechanisms to protect the integrity of D_CONFIG_KEYS, D_CRYPTO_KEYS, D_MANAGEMENT, |

| Objective | Description |
|---|---|
| | D_CONFIG_MANAGEMENT or D_AUDIT. |
| **O_ROLES** | The TOE shall provide a user management function, which allows defining users for operation and administration based on the general privilege categories listed in Table *1*.4. |

***Table 4.1: Security Objectives for the TOE***

## 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.

| Objective | Description |
|---|---|
| **OE_ADMIN** | The OE shall ensure that users are properly trained to perform TOE tasks according to their role.<br>Administrators shall be trained to configure and supervise the TOE and its security functions. |
| **OE_AUDIT** | The OE shall ensure that users monitor alarms and an administrative user regularly reviews SNMP Logs and security event logs. The TOE shall also ensure that appropriate corrective actions, according to Alcatel-Lucent recommendations for managing the TOE, are taken upon potential incident detection. |
| **OE_CONFIGURATION** | The OE shall ensure that the TOE is installed and commissioned following Alcatel-Lucent recommendations and procedures in order to properly protect the primary and secondary assets of the TOE.<br>The OE shall ensure that Neighboring Equipment, non-TOE components are configured following the vendor security recommendations and settings. |
| **OE_ORGANIZATION** | The OE and all employees shall follow the organizational policies, guidelines and procedures. |
| **OE_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. It is also assumed that non-TOE management assets and the Neighboring Equipment have at least the same level of physical and logical protection as the TOE.<br>Furthermore, the OE shall protect data intended for transmission to the TOE including D_DATA and the defined secondary assets. The OE shall handle data originating from the TOE securely. |

***Table 4.2: Environmental Security Objectives for the TOE***

## 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.

| Assumption, Threat or OSP | Security Objective | Rationale |
|---|---|---|
| **A_ADMIN** | **OE_ADMIN** | OE_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_ADMIN particularizes the training concepts for administrators and crypto officers. Therefore, the assumption A_ADMIN is covered by the security objective OE_ADMIN. |
| **A_AUDIT** | **OE_AUDIT** | OE_AUDIT requires the user to monitor alarms and an administrative user to regularly review SNMP Logs and security event logsas assumed in A_AUDIT. Also OE_AUDIT requires that appropriate corrective actions, according to Alcatel-Lucent recommendations for managing the TOE are taken upon potential incident detection as assumed in A_AUDIT. Therefore, the assumption is covered by the objective. |
| **A_CONFIGURATION** | **OE_ CONFIGURATION** | OE_CONFIGURATION covers what is assumed in A_CONFIGURATION, since it requires that the TOE is installed and commissioned following Alcatel-Lucent recommendations and procedures in order to properly protect the primary and secondary assets of the TOE. In addition, OE_CONFIGURATION requires that Neighboring Equipment, non-TOE components are configured following the vendor security recommendations and settings. |
| **A_ORGANIZATION** | **OE_ORGANIZATION** | OE_ORGANIZATION requires the operational environment and employees to follow organizational policies, guidelines and procedures as assumed in A_ORGANIZATION. |

| Assumption, Threat or OSP | Security Objective | Rationale |
|---|---|---|
| **A_PROTECTION** | **OE_PROTECTION** | OE_PROTECTION requires that the TOE is located in a controlled and secured zone in order to prevent unauthorized logical and physical access. OE_PROTECTION also requires that non-TOE management assets and the Neighboring Equipment have at least the same level of physical and logical protection as the TOE. Furthermore, OE_PROTECTION requires that data intended for transmission to the TOE including D_DATA and the defined secondary assets are protected. It is also required that data originating from the TOE is securely handled. These requisitions are assumed in A_PROTECTION. |
| **T_DATA_DISCLOSURE** | **O_DATA_ CONFIDENTIALITY** | The threat T_DATA_DISCLOSURE is averted by the security objective O_DATA_CONFIDENTIALITY. |
| **T_CONFIG_ EXTRACTION** | **O_MANAGEMENT_ CONFIDENTIALITY** | The threat T_CONFIG_EXTRACTION is averted by the security objective O_MANAGEMENT_CONFIDENTIALITY. |
| **T_CONFIG_ MODIFICATION** | **O_MANAGEMENT_ PROTECTION** | The threat T_CONFIG_MODIFICATION is averted by the security objective O_MANAGEMENT_PROTECTION. |
| **OSP_ACCESS** | **O_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. Therefore, OSP_ACCESS is covered by O_ACCESS. |
| **OSP_ALARM** | **O_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). |

| Assumption, Threat or OSP | Security Objective | Rationale |
|---|---|---|
| **OSP_AUDIT** | **O_AUDIT** | Since O_AUDIT requires the TOE to provide SNMP Logs and security event 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.Therefore, it covers OSP_AUDIT which requires tracking configuration changes so that users can be made accountable. |
| **OSP_CRYPTO** | **O_CRYPTO_ CONFORMITY** | O_CRYPTO_CONFORMITY requires the TOE to provide conformity for D_DATA encryption and decryption following FIPS 140-2 Level 2. Since OSP_CRYPTO requires an internationally accepted cryptographic standard, OSP_CRYPTO is covered by O_CRYPTO_CONFORMITY. |
| **OSP_KEY_ MANAGEMENT** | **O_KEY_ MANAGEMENT** | O_KEY_MANAGEMENT exactly requires the provision of mechanisms and procedures that allow authenticated and authorized users to securely configure and manage D_CRYPTO_KEYS and D_CONFIG_KEYS, what is described in OSP_KEY_MANAGEMENT. |
| **OSP_MANAGEMENT** | **O_MANAGEMENT** | O_MANAGEMENT requires the TOE to provide a management capability that allows authenticated and authorized users to manage the equipment and its cryptographic functions. Since OSP_MANAGEMENT requires that the TOE provides a management capability for the equipment and its cryptographic functions, OSP_MANAGEMENT is covered by O_MANAGEMENT. |
| **OSP_ROLES** | **O_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_ROLES requires a role management function which allows the assignment of different authorization levels for administration and operation. Therefore, OSP_ROLES is covered by O_ROLES. |

***Table 4.3: Security Objective Rationale***

| Threats | OSPs | Assumptions |
|---|---|---|

| | T_DATA_DISCLOSURE | T_CONFIG_EXTRACTION | T_CONFIG_MDODIFICATION | OSP_ACCESS | OSP_ALARM | OSP_AUDIT | OSP_CRYPTO | OSP_MANAGEMENT | OSP_KEY_MANAGEMENT | OSP_ROLES | A_ADMIN | A_AUDIT | A_CONFIGURATION | A_ORGANISATION | A_PROTECTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O_DATA_CONFIDENTIALITY | X | | | | | | | | | | | | | | |
| O_MANAGEMENT_CONFIDENTIALITY | | X | | | | | | | | | | | | | |
| O_MANAGEMENT_PROTECTION | | | X | | | | | | | | | | | | |
| O_ACCESS | | | | X | | | | | | | | | | | |
| O_ALARM | | | | | X | | | | | | | | | | |
| O_AUDIT | | | | | | X | | | | | | | | | |
| O_CRYPTO_CONFORMITY | | | | | | | X | | | | | | | | |
| O_MANAGEMENT | | | | | | | | X | | | | | | | |
| O_KEY_MANAGEMENT | | | | | | | | | X | | | | | | |
| O_ROLES | | | | | | | | | | X | | | | | |
| OE_ADMIN | | | | | | | | | | | X | | | | |
| OE_AUDIT | | | | | | | | | | | | X | | | |
| OE_CONFIGURATION | | | | | | | | | | | | | X | | |
| OE_ORGANIZATION | | | | | | | | | | | | | | X | |
| OE_PROTECTION | | | | | | | | | | | | | | | X |

***Table 4.4: Security Objective Mapping***

# 5. Extended Components Definition

## 5.1 Extended TOE Security Functional Components

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

### 5.1.1 Class FAU: Security Audit

The FAU class, as defined in CC Part 2, addresses requirements for security auditing.

#### 5.1.1.1 FAU_STG

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

5.1.1.1.1 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. |
| | Depedencies: 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, TLS, TLS/HTTPS, SNMPv3] protocol. |

## 5.2 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).

The table provided below is a summary of the operations performed on the security functional requirements selected for the TOE. The operations will be identified as follows: A = Assignment, S = Selection, R = Refinement and I = Iteration.

| Class | SFR | A | S | R | I |
|---|---|---|---|---|---|
| **Security Audit** | **FAU_ARP.1** Security alarms | X | | X | |
| | **FAU_GEN.1** Audit data generation | X | X | | |
| | **FAU_GEN.2** User identity association | | | | |
| | **FAU_SAA.1** Potential violation analysis | X | | | |
| | **FAU_STG_EXT.1** External audit trail storage | | X | | |
| **Cryptographic Support** | **FCS_CKM.4** Cryptographic key destruction | X | | | |
| | **FCS_COP.1(1)** Cryptographic operation | X | | | X |
| | **FCS_COP.1(2)** Cryptographic operation | X | | X | X |
| **User Data Protection** | **FDP_ACC.1** Subset access control | X | | | |
| | **FDP_ACF.1** Security attribute based access control | X | | | |
| | **FDP_ITC.1** Import of user data without security attributes | X | | | |
| **Identification and Authentication** | **FIA_UAU.2** User authentication before any action | | | | |
| | **FIA_UID.2** User identification before any action | | | | |
| **Security Management** | **FMT_SMF.1** Specification of management functions | X | | | |
| | **FMT_SMR.1** Security roles | X | | | |
| **Protection of the TSF** | **FPT_STM.1** Reliable time stamps | | | | |
| **Trusted Path/Channels** | **FTP_ITC.1** Inter-TSF trusted channel | X | X | | |

***Table 6.1: Security Functional Requirements***

### 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;
- Use of the defined management functions;
- Unsuccessful login;
- Key destruction;
- Configure and manage cryptographic keys; and
- Successful import of user data (keys)].

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 user name and the action itself; and
- The Security Auditing Alarms will contain information about DWDM transmission errors].

Hierarchical to: No other components.
Dependencies: 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: No other components.
Dependencies: 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: No other components.
Dependencies: 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 [Alcatel’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(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 800-67)] and cryptographic key sizes [256 binary digits in length] that meet the following: [FIPS 140-2 Level 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<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_COP.1(2)** | **Cryptographic operation** |
| FCS_COP.1.1(2) | The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [HMAC-SHA-1] ~~and cryptographic~~ key sizes [40 bits] **and message digest sizes 96 bits** that meet the following: [FIPS 198-1 and FIPS 180-3]. |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes,<br>or<br>FDP_ITC.2 Import of user data with security attributes,<br>or<br>FCS_CKM.1 Cryptographic key generation]<br>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 [<br>• Subjects: Users or processes attempting to perform management functions using an SNMP MIB<br>• Objects: MIBs<br>• Operations: read-view, write-view, notify-view]. |
| Hierarchical to: | No other components. |
| Dependencies: | 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 authorise access of subjects to objects based on the following additional rules: [

- None].

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

- None].

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

**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 initialisation

### 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:<br>Dependencies: | FIA_UAU.1 Timing of authentication.<br>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:<br>Dependencies: | FIA_UID.1 Timing of identification.<br>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: [<br>- Management of advanced equipment and service management functions.<br>- Management of restricted equipment and service management functions.<br>- Management of the configuration of IO cards, ports, interfaces and circuits.<br>- Management of user information retrieval.<br>- Management of security and privilege information.<br>- Management of D_MANAGEMENT and D_CONFIG_MANAGEMENT.<br>- Management of encryption state and cryptographic functions.<br>- Management of test procedures on any card that does not contribute to system-wide outage.<br>- Management of system-wide tests.<br>- Management of actions that require trusted channel support.<br>- Defining the external IT entity to which audit data is transferred.]. |
| Hierarchical to:<br>Dependencies: | No other components.<br>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. |

### 6.1.7 Trusted Path/Channels (FTP)

| | |
|---|---|
| **FTP_ITC.1** | **Inter-TSF trusted channel** |
| FTP_ITC.1.1 | The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. |
| FTP_ITC.1.2 | The TSF shall permit [*the TSF or another trusted IT product*] to initiate communication via the trusted channel. |
| FTP_ITC.1.3 | The TSF shall initiate communication via the trusted channel for [<br>- administration and operation of the TOE<br>- management of the cryptographic functions of the TOE<br>- transmission of secondary assets]. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

## 6.2 Security Assurance Requirements

The following Table lists all security assurance components that are valid for this Security Target. All these security assurance components are required by EAL2 augmented with ALC_FLR.2.

| Class | Component |
|---|---|
| **Development** | **ADV_ARC.1** Security architecture description |
| | **ADV_FSP.2** Security-enforcing functional specification |
| | **ADV_TDS.1** Basic design |
| **Guidance Documents** | **AGD_OPE.1** Operational user guidance |
| | **AGD_PRE.1** Preparative procedures |
| **Lifecycle Support** | **ALC_CMC.2** Use of a CM system |

| Class | Component |
|---|---|
| | **ALC_CMS.2** Parts of the TOE CM coverage |
| | **ALC_DEL.1** Delivery procedures |
| | **ALC_FLR.2** Flaw reporting procedures |
| **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.1** Evidence of coverage |
| | **ATE_FUN.1** Functional testing |
| | **ATE_IND.2** Independent testing - sample |
| **Vulnerability Assessment** | **AVA_VAN.2** Vulnerability analysis |

***Table 6.2: 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_KEY_MANAGEMENT | O_MANAGEMENT_CONFIDENTIALITY | O_MANAGEMENT_PROTECTION | O_ROLES |
|---|---|---|---|---|---|---|---|---|---|---|
| **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 | | | X | X | |
| **FCS_COP.1(2)** Cryptographic operation | | | | | | | | X | X | |
| **FDP_ACC.1** Subset access control | | | | X | X | X | X | | | |
| **FDP_ACF.1** Security attribute based access | | | | X | X | X | X | | | |

| | O_ACCESS | O_ALARM | O_AUDIT | O_CRYPTO_CONFORMITY | O_DATA_CONFIDENTIALITY | O_MANAGEMENT | O_KEY_MANAGEMENT | O_MANAGEMENT_CONFIDENTIALITY | O_MANAGEMENT_PROTECTION | O_ROLES |
|---|---|---|---|---|---|---|---|---|---|---|
| control | | | | | | | | | | |
| **FDP_ITC.1** Import of user data without security attributes | | | | X | X | | | | | |
| **FIA_UAU.2** User authentication before any action | X | | X | | | X | X | | | |
| **FIA_UID.2** User identification before any action | X | | X | | | X | X | | | 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 | | | | | | | |
| **FTP_ITC.1** Inter-TSF trusted channel | | | | | | | | X | X | |

***Table 6.3: 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.<br>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 functional requirement FAU_ARP.1 requires that the user will be notified upon detection of a potential security violation. Therefore, 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. Since O_ALARM requires the TOE to notify the User about potential intrusion events, these security functional requirements are suitable to meet the security objective. |
| **O_AUDIT** | O_AUDIT requires the TOE to provide SNMP Logs and security event 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 as defined by FIA_UID.2.The SFR FAU_STG_ET.1 requires audit records be sent to an external IT entity for storage and viewing. All SFRs mentioned exactly require to implement SNMP Logs and security event logs as defined by O_AUDIT. |

| Security Objective(s) | Rationale |
|---|---|
| **O_CRYPTO_CONFORMITY**<br>**O_DATA_CONFIDENTIALITY** | The security requirement FCS_COP.1(1) defines the cryptographic operations, encryption and decryption, in more detail. AES 256 that meet the FIPS 140-2 L2 standard shall be provided. FCS_COP.1(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.. Therefore, these SFRs fulfill O_CRYPTO_CONFORMITY which provides conformity for D_DATA encryption and decryption following the requirements defined by FIPS 140-2 Level 2.<br>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.<br>O_DATA_CONFIDENTIALITY requires the TOE to protect the confidentiality of D_DATA. Exactly this is fulfilled by the security functional requirements FCS_COP.1(1) and its dependent SFRs, since they provide encryption and decryption of data as discussed above. |

| Security Objective(s) | Rationale |
|---|---|
| **O_KEY_MANAGEMENT**<br>**O_MANAGEMENT** | O_KEY_MANAGEMENT and O_MANAGEMENT require 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.<br>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.<br>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. |
| **O_MANAGEMENT_CONFIDENTIALITY**<br>**O_MANAGEMENT_PROTECTION** | O_MANAGEMENT_CONFIDENTIALITY and O_MANAGEMENT_PROTECTION require the provision of mechanisms to protect the confidentiality and integrity of D_CRYPTO_KEYS, D_CONFIG_KEYS, D_AUDIT, D_CONFIG_MANAGEMENT and D_MANAGEMENT.<br>The security functional requirement FTP_ITC.1 requires the TOE to implement a trusted communication channel between the TSF and the NMS or KMT management tools.<br>SNMPv3 in AuthPriv mode will be used to establish this trusted communication channel. The algorithms specified in Table 1.3are defined in FCS_COP.1(1) and FCS_COP.1(2). The algorithm certificates awarded by the CAVP are identified in Table 8.1. |
| **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. |

***Table 6.4: 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<br>FIA_UID.1 | FAU_GEN.1<br>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]<br>FCS_CKM.4 | FDP_ITC.1<br>FCS_CKM.4 |
| FCS_COP.1(2) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]<br>FCS_CKM.4 | FDP_ITC.1<br>FCS_CKM.4 |
| FDP_ACC.1 | FDP_ACF.1 | FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | FDP_ACC.1<br>See discussion below. |
| FDP_ITC.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_MSA.3 | FDP_ACC.1<br>See discussion below |
| FIA_UAU.2 | FIA_UID.1 | FIA_UID.2 |
| FIA_UID.2 | -- | -- |
| FMT_SMF.1 | -- | -- |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 |
| FPT_STM.1 | -- | -- |
| FTP_ITC.1 | -- | -- |

*Table 6.5: 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.

### 6.3.3 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile location and embedded in or protected by other products designed to address threats that correspond with the intended environment. ALC_FLR.2 was added to provide assurance that the vendor will respond to reports of new threats and reported defects in the TOE.

### 6.3.4 Explicitly-Defined Security Functional Requirements Rationale

CC Part 2 does not define an SFR for requiring the TOE to transmit audit data to an external IT entity, so this ST defines FAU_STG_EXT.1..

# 7. TOE Summary Specification

The TOE provides the following security services:

- Cryptographic Support
- Secure Management
- User Authentication, Authorization and Audit Logs
- Potential Intrusion Alarms

## 7.1.1 Cryptographic Support

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 contains two implementations of AES:<br>1) The 11QPEN4 encryption card contains a FPGA which will encrypt all traffic on the four optical fiber interfaces. This implementation has been awarded algorithm certificate number #2828 by the CAVP.<br>2) A separate AES implementation is used by the NE-NMS and NE-KMT management interfaces. This implementation has been awarded the following algorithm certificates by the CAVP:<br>PSS4 Crypto-SNMP Engine<br>AES256: #2829<br>PSS32/16 Crypto-SNMP Engine<br>AES256: #2830 |
| **FCS_COP.1(2)** | The TOE contains implementations of SHS and HMAC which are used by the NE-NMS and NE-KMT management interfaces.<br>The following algorithm certificate numbers have been awarded by the CAVP:<br>PSS4 Crypto-SNMP Engine<br>SHA1: #2370<br>HMAC: #1770<br>CVL: #255<br>PSS32/16 Crypto-SNMP Engine<br>SHA1: #2371<br>HMAC: #1771<br>CVL: #256 |
| **FCS_CKM.4** | The TOE has been validated to FIPS 140-2 and awarded Cert# TBD by the CMVP for Security Level 2.<br>Therefore the TOE implements the destruction of cryptographic keys. |

***Table 7.1: Rationale For Cryptographic Support***

### 7.1.2 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**<br>**FDP_ACF.1**<br>**FDP_ITC.1** | The access to management and encryption functions is only possible after successful user authentication and authorization as an Administrator.<br>The 11QPEN4 Session Encryption Key is an AES-256 key that is imported across an encrypted SNMPv3 link from the KMT. |
| **FMT_SMF.1** | An important part of the TOE configuration is the transformation of the system from Default Mode to FIPS Mode, during which the Secure Management interfaces (NE-NMS and NE-KMT), authentication parameters and other security settings are configured. The initialization of the keys for the Secure Management interfaces is done out-of-band and using pre-shared keys.<br>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).<br>Refer to Table *1*.4: User Roles for a list of the functions that can be performed by each role. |
| **FTP_ITC.1** | Management of the TOE can only be performed via the NE-NMS and NE-KMT interfaces which use SNMPv3 in AuthPriv mode with the following settings:<br>• Authentication: HMAC-SHA-1-96<br>• Privacy: AES 256 (CFB128 mode) |

***Table 7.2: Rationale for Secure Management***

### 7.1.3 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 and the security event log.

| SFR(s) | Rationale |
|---|---|

| SFR(s) | Rationale |
|---|---|
| **FAU_GEN.1**<br>**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.<br>The TOE also records the important security relevant events not resulting directly from an SNMP request in the security event log.<br>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**<br>**FIA_UID.2** | 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. |
| **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***

### 7.1.4 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**<br>**FAU_SAA.1** | The TOE implements the following for the detection of a potential intrusion or an attempt to hide another type of attack:<br>• DWDM transmission alarm<br>○ Will detect potential attempts to gain physical access to the optical fiber.<br>○ 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***

# 8. Abbreviations, Terminology and References

## 8.1 Abbreviations

The following abbreviations are used in this document.

| Term | Description |
|---|---|
| **AES** | Advanced Encryption Standard |
| **DWDM** | Dense Wave Division Multiplexing |
| **CAVP** | Cryptographic Algorithm Validation Program |
| **CBC** | Cipher-Block Chaining |
| **CC** | Common Criteria |
| **CMVP** | Cryptographic Module Validation Program |
| **CTR** | Counter Mode |
| **DoS** | Denial of Service |
| **EAL** | Evaluation Assurance Level |
| **EC** | Equipment Controller |
| **FC** | Fiber Channel |
| **FIPS** | Federal Information Processing Standard |
| **FPGA** | Field Programmable Gate Array |
| **GE** | Gigabit Ethernet |
| **HMAC** | Keyed-Hash Message Authentication Code |
| **IPsec** | Internet Protocol security |
| **KMT** | Key Management Tool |
| **NE** | Network Element |
| **NMS** | Network Management System |
| **NTP** | Network Time Protocol |
| **OSP** | Organisational Security Policy |
| **OTU** | Optical Transport Unit |
| **PSS** | Photonic Service Switch |
| **QPEN** | Quad  Port Encryption Transponder |
| **RBAC** | Role Based Access Control |
| **SFTP** | Secure File Transfer Protocol |
| **SHS** | Secure Hash Standard |
| **SLA** | Service Level Agreement |
| **SSH** | Secure Shell |
| **SSL** | Secure Socket Layer |
| **SNMP** | Secure Network Management Protocol |
| **TLS** | Transport Layer Security |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **uBCM** | Micro Board Control Module |
| **Web-UI** | Web User Interface |
| **XFP** | 10 Gigabit Small Form Factor Pluggable |

***Table 8.1: Abbreviations***

## 8.2 Terminology

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

## 8.3 References

| Abbreviation | Document |
|---|---|
| **[CC]** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, CCMB-2012-09-(001 to 003) |
| **[CCP1]** | Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, July 2012 |
| **[CCP2]** | Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 |
| **[CCP3]** | Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 |
| **[CEM]** | Common Methodology for Information Technology Security Evaluation; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 |
| **[FIPS_1]** | 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 |

***Table 8.2: References***

END OF DOCUMENT