FiberHome Enhanced Optical Transport Equipment Manager Security Target

Version: 1.9

FiberHome Telecommunication Technologies Co., Ltd.

September 2021

LEGAL INFORMATION

Document History

Table 1 - History of FiberHome Enhanced Optical Transport Equipment Security Target

Version	Date	Description
1.0	2020/06/22	Initial version
1.1	2020/07/03	Update TOE name and Webpage link
1.2	2020/9/17	Revision of the assessment
1.3	2020/9/18	Revise the format
1.4	2020/9/25	Add Security related card and Non-Security related card
1.5	2020/12/18	Revision Comments
1.6	2021/3/9	Revision Comments
1.7	2021/05/06	Revision Comments
1.8	2021/09/02	Revision Comments
1.9	2021/09/27	Revision Comments

Contents

1 ST Introduction..... 7

1.1 ST reference.....7

1.2 TOE reference..... 7

1.3 TOE Overview.....7

1.3.1 TOE Type.....10

1.3.2 Major features of the TOE..... 10

1.3.3 Required non-TOE hardware/software/firmware..... 10

1.4 TOE Description.....11

1.4.1 Evaluated configuration..... 11

1.4.2 Physical Scope..... 12

1.4.3 Logical Scope.....16

2 Conformance Claims.....17

2.1 CC conformance claim..... 17

2.2 PP claim.....17

2.3 Security requirement package claim..... 17

3 Security Problem Definition..... 18

3.1 Threats..... 18

3.1.1 Assets and threat agents..... 18

3.1.2 Threats.....18

3.2 Organizational Security Policies..... 19

3.3 Assumptions..... 19

4 Security Objectives.....20

4.1 Security Objectives for the TOE..... 20

4.2 Security Objectives for the Environment..... 21

5 Extended Component Definition.....23

6 IT Security Requirements.....25

6.1 Security Functional Requirements..... 25

6.1.1 Access..... 26

6.1.2 Identification & Authentication..... 27

6.1.3 Roles &Authorisation..... 29

6.1.4 Logging & Auditing.....31

6.1.5 Protection of the TSF.....32

6.1.6 Management.....32

6.2 Security Assurance Requirements.....34

6.3 Security Assurance Requirements Rationale.....36

7 TOE Summary Specification.....37

8 Rationale.....41

8.1 Rationale for Security Objectives.....41

8.2 Security Functional Requirements Rationale.....45

8.2.1 Dependencies Rationale.....49

9 Appendix..... 51

9.1 Acronyms..... 51

9.2 References..... 51

Figures

Figure 1 - TOE demarcation.....9

Tables

Table 1 - History of FiberHome Enhanced Optical Transport Equipment Security Target.....3

Table 2 – UNM2000 EMS Server requirements..... 10

Table 3 – UNM2000 EMS Client requirements..... 11

Table 4 - Physical scope of optical transport equipment.....12

Table 5 - Physical scope of UNM2000 EMS Server.....14

Table 6 - Physical scope of UNM2000 EMS Client.....15

Table 7 - TOE security functional requirements.....25

Table 9 – Management functions.....32

Table 10 – Security Assurance Requirements..... 34

Table 11 – Rationale for security objectives (1).....41

Table 12 – Rationale for security objectives (2).....42

Table 13 – Rationale for SFRs (1).....45

Table 14 - Rationale for SFRs (2).....46

Table 12 - Rationale for dependencies of security functional requirements..... 49

1 ST Introduction

1.1 ST reference

ST title: FiberHome Enhanced Optical Transport Equipment Manager Security Target

ST developer: FiberHome Telecommunication Technologies Co., Ltd.

ST version number: 1.9

1.2 TOE reference

TOE name: FiberHome Enhanced Optical Transport Equipment Manager including UNM2000 Server and UNM2000 Client and OTEs: FONST1000 D2, FONST 5000 COTP, FONST 5000 U10E, FONST 5000 U20E, and FONST 5000 N32.

TOE version: UNM2000 EMS Server version V3R2SP1

UNM2000 EMS Client version V3R2SP1

FONST 5000 COTP version RP0100

FONST 5000 U10E version RP0101

FONST 5000 U20E version RP0101

FONST 1000 D2 version RP0100

FONST 5000 N32 version RP0101

1.3 TOE Overview

This chapter presents a general overview of FiberHome Enhanced Optical Transport Equipment Manager, a distributed TOE for the management of the Optical Network Terminal (ONT) equipment used to terminate the optical fiber line, demultiplex the signal into its component parts (voice telephone, television, and Internet), and provide power to customer telephones. FiberHome Enhanced Optical Transport Equipment also helps to provide secure Internet connectivity.

The TOE is deployed in three parts:

UNM2000 Element Management System (EMS) server

UNM2000 Element Management System (EMS) client

Optical Transport Equipment (OTE), namely FONST

FONST stands for company product series name, following 4 digit numbers was decided by physical size, and following identification code means different scenario was described as follow:

No	TOE	Description
1	FONST 5000 COTP	The COTP is an optical layer subrack, Which is a single-layer single-sided subrack providing full-height and half-height slots.
2	FONST 5000 U10E	U10E is an electrical layer subfrack for OTN electrical layer board access, it has 11 service slots and a backplane bandwidth of 400G/per slot.
3	FONST 5000 U20E	U20E is an electrical layer subfrack for OTN electrical layer board access, it has 22 service slots and a backplane bandwidth of 400G/per slot.
4	FONST 1000 D2	The FONST 1000 D2 is data center interconnection equipment. It features small size, large capacity, high speed, low power consumption, and optical / electrical integration. It has 8 service slots and the maximum capacity of a single slot is 800G.
5	FONST 5000 N32	The FONST 5000 N32 integrated sub rack is three-layered and single-sided. It has 32 service slots and the maximum capacity of a single slot is 400G.

The TOE through the application of OTN technology guarantees the flexibility of service end-to-end (E2E) grooming and enables different services to share bandwidth. The network maintenance and fault isolation can be performed easily by virtue of abundant OTN overheads and simple operation on the EMS.

The TOE is depicted with red dashed line in Figure 1, together with relevant entities in its

environment.

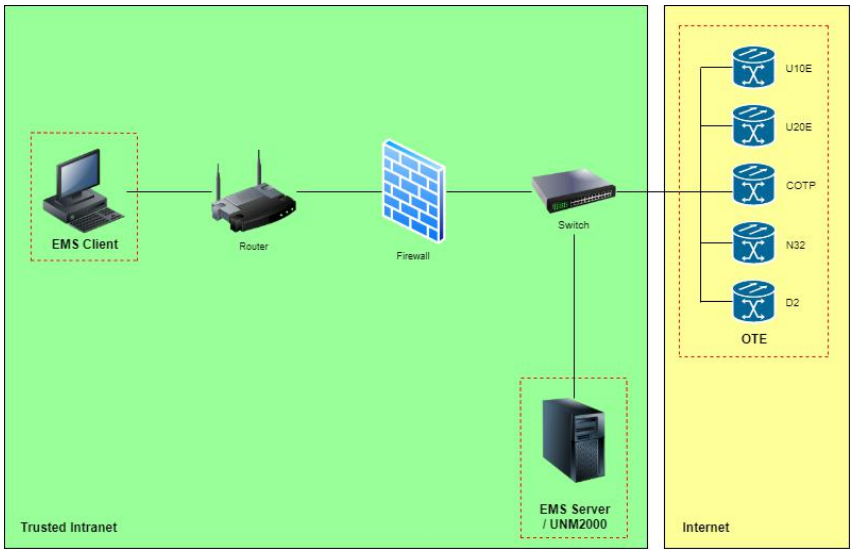


Figure 1 - TOE demarcation

The structure of the deployed TOE, including its role in the system is as follows:

The UNM2000 EMS Client and the UNM2000 EMS Server parts of the TOE are connected to the same Intranet, which is considered trusted.

The OTEs (also part of the TOE) are distributed and connected to Internet.

The UNM2000 EMS Server sends performance data, alarm data, configuration data and similar information to the OTE.

One or more management workstations with an UNM2000 EMS Client installed on them, which is used as a graphical user interface to the EMS Server.

The Operating System Windows Server 2012 of the UNM2000 EMS server supply timestamps.

The communication between the UNM2000 EMS Server and the OTEs is done using a private protocol based on TCP/IP with a different encapsulation format.

Lastly, the TOE uses a MYSQL 14.14 in order to store the user credentials and the logs. This database is located in the UNM2000 EMS Server and it is installed at the same time that the EMS Server software, therefore, no additional configuration is required. This database has no direct interface associated and its protection is ensured by the TOE environment.

1.3.1 TOE Type

The TOE is a distributed solution for the management of OTEs (models FONST1000 D2, FONST 5000 COTP, FONST 5000 U10E, FONST 5000 U20E, and FONST 5000 N32). The TOE encompasses:

The software running on the UNM2000 EMS Server

The software running on the UNM2000 EMS Client

The firmware running on the OTEs

All the security functionality of the TOE relies on the software/firmware. No security functionality relies on the hardware.

1.3.2 Major features of the TOE

The major security features of the TOE are the following:

Authentication: the TOE implements mechanisms for users authentication

Authorization: the TOE implements a role-based access control policy for users

Access Control: the TOE control the access to the OTEs

Audit: the TOE generates audit records

Management: the TOE include management functionality

1.3.3 Required non-TOE hardware/software/firmware

The UNM2000 EMS Server requires for its operation:

Table 2 – UNM2000 EMS Server requirements

Type	Name and version
Hardware	A Server suitable to run the OS. Suggested Hardware: CPU 4 E5-2667V2-8 core Processors RAM Memory 128GB 6 x 600 GB physical hard disk 2 x 200G SSD + 30T disk array

Type	Name and version
OS	Windows Server 2012 R2 (Supply time sources)
Database	MYSQL 14.14 distribution 5.7.18 for Win64 (x86_64)

The UNM2000 EMS Client requires for its operation:

Table 3 – UNM2000 EMS Client requirements

Type	Name and version
Hardware	A Workstation suitable to run the OS. Suggested Hardware: CPU Intel XeonE5-2637V2 (4-core) 3.5GHz RAM Memory 16GB 1 x 2TB physical hard disk
OS	Windows 10 (10.0.10240)

1.4 TOE Description

1.4.1 Evaluated configuration

The evaluated configuration of the TOE consist of:

UNM2000 EMS Server

Hardware

Same hardware as defined in section 1.3.3 Required non-TOE hardware/software/firmware

Software

Windows Server 2012 R2

TOE – UNM2000 EMS Server V3R2SP1

UNM2000 EMS Client

Hardware

Same hardware as defined in section 1.3.3 Required non-TOE hardware/software/firmware

Software

Windows 10 (10.0.10240)

TOE – UNM2000 EMS Client V3R2SP1

OTEs

FONST1000 D2, FONST 5000 COTP, FONST 5000 U10E, FONST 5000 U20E, and FONST 5000 N32

1.4.2 Physical Scope

1.4.2.1 Physical Scope Optical Transport Equipment

Table 4 - Physical scope of optical transport equipment

Type	Identifier	Version	Form of Delivery	Developer	Hash
HW	FONST 5000 COTP	RP0100	package module	FiberHome	
	FONST 5000 U10E	RP0101		FiberHome	
	FONST 5000 U20E	RP0101		FiberHome	
	FONST 1000 D2	RP0100		FiberHome	
	FONST 5000 N32	RP0101		FiberHome	
PDF	FONST 1000 D2 Data Center Interconnection Equipment Configuration Guide	A	fhm.FiberHome.com	FiberHome	85ab3b3ab0bfd18d5c8fe065847b99e654dd1ff39d190c6c21cd46bb7417afd6
	FONST 1000 D2 Data Center Interconnection Equipment Hardware Description	A	fhm.FiberHome.com	FiberHome	8b815af66b3885c6130cc7636b6635db90cbcaa3f48659cbdbc61e2dfaed7107

Type	Identifier	Version	Form of Delivery	Developer	Hash
	FONST 1000 D2 Data Center Interconnection Equipment Product Description	A	fhm.FiberHome.com	FiberHome	03d1656e955f8467dc317d589008c32474587370ef048610ce9f083ff3d3495c
	FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description	I	fhm.FiberHome.com	FiberHome	898a22d86caf2de7bcc78135ca456d2921bca60eb3124b34d09eff63beadcaa7
	FONST 5000 U Series Packet Enhanced OTN Equipment Product Description	I	fhm.FiberHome.com	FiberHome	b10b1c1fa5e4cf14e504b302d585ba38bd03fac031c25dc13b58e40400e1860e
	FONST 5000 U Series Packet Enhanced OTN Equipment Troubleshooting Guide	B	fhm.FiberHome.com	FiberHome	4d62bc48cf34fa92f7c8dee273ae703d87e59327a1d2d3bc7ada4d9a00f1fb1f
	POTN Series of Products Handling of Common Alarms	A	fhm.FiberHome.com	FiberHome	0cd5ee7af1bb7a60541438c2b72788aa530a4203986b8151e3ae4bf7ede7a9bb

1.4.2.2 Physical Scope UNM2000 EMS Server

Table 5 - Physical scope of UNM2000 EMS Server

Type / Name		Version	Form of Delivery	Developer	Hash
Hardware	UNM2000 Element Management System Server equipment	N.A.	package module	FiberHome	
Software	UNM2000 Element Management System Server software	UNM2000 V3R2SP1	Pre-installed	FiberHome	
PDF	UNM2000_Network Convergence Management System V3R2 Operation Guide	A	fhm.FiberHome.com	FiberHome	3e1ae16516e08ccf818f207dcdb2253ea3fcfd2038c596a63335f0263b25c746
	UNM2000_Network Convergence Management System V3R2_Release Notes	A	fhm.FiberHome.com	FiberHome	f84889f7f652da3572196d325d01455cc84cdcf5baa39b8e136507ab5ee29a01
	UNM2000_Network Convergence Management System V3R2 Installation Guide	A	fhm.FiberHome.com	FiberHome	fbeb71cbd1128ff46506488c577b52273c116753e01bfda8014b8cab5c113e55
	UNM 2000 OTN POTN Service Configuration Guide	A	fhm.FiberHome.com	FiberHome	fff30b677b8a2cdb921da99be55742d720e77269cf6ee34edf918f

Type / Name		Version	Form of Delivery	Developer	Hash
					d1177ec3ce
	UNM2000_Network Convergence Management System Troubleshooting Guide	A	fhm.FiberHome.com	FiberHome	d17889cc7f499886666136922d43df5ea33622d8dec15a5e1c9adb48e24b49ef

1.4.2.3 Physical scope UNM2000 EMS client

Table 6 - Physical scope of UNM2000 EMS Client

Type	Name	Version	Form of Delivery	Developer	Hash
Software	UNM2000 Element Management System Client software	V3R2SP1	CD-ROM	FiberHome	85ab3b3ab0bfd18d5c8fe065847b99e654dd1ff39d190c6c21cd46bb7417afd6
PDF	Please refer to Guide regarding UNM2000 EMS Server	NA	Together with UNM2000 EMS Server package.	FiberHome	

1.4.3 Logical Scope

The TOE logical scope consists of the security functions/features provided/controlled by the TOE. The TOE provides the following security features:

1.4.3.1 Authentication

The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users from UNM2000 EMS client based on: username/password and a configurable subset of IP address and time of login.

1.4.3.2 Authorization

The TOE supports a flexible role-based authorization framework with predefined and customizable roles for management. These roles can use the UNM2000 EMS server to manage OTEs.

1.4.3.3 Access Control

OTE transport data of WDM/OTN/POTN/DCI connecting status, in such a way that:

Only the intended recipients from UNM2000 EMS server are able to read OTE signal.

Nobody can modify the signals of OTE, which was monitored by UNM2000 EMS server.

1.4.3.4 Audit

UNM2000 EMS server supports flexible logging and auditing of events.

Records in log files can provide the following uses: monitoring system resources; auditing user behaviour; alerting on suspicious behaviour.

1.4.3.5 Management

The TOE manages traffic rules, authentication, authorization, user accounts and sessions.

2 Conformance Claims

2.1 CC conformance claim

This ST claims conformance to

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001/2/3, Version 3.1, Revision 5, April 2017.

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-001/2/3, Version 3.1, Revision 5, April 2017.

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-001/2/3, Version 3.1, Revision 5, April 2017.

as follows

CC Part 2 extended,

CC Part 3 conformant.

2.2 PP claim

This security target does not claim to any protection profile.

2.3 Security requirement package claim

This security target claims to be conformant to the assurance package **EAL 2** augmented by **ALC_FLR.2** (Flaw reporting procedures).

3 Security Problem Definition

3.1 Threats

3.1.1 Assets and threat agents

The assets are:

1. **A.Security_parameter**: Security parameter's confidentiality and integrity that was set by administrators in UNM2000 EMS Server.
2. **A.OTE_communication**: Confidentiality and integrity of communication between OTE and UNM2000 EMS server.

These assets are threatened by the following threat agents:

1. **TA.ACCESS_OTE**: An attacker with access to OTEs.
2. **TA.PHYSICAL**: An attacker with physical access to the UNM2000 EMS server.
3. **TA.ROGUE_USER**: A user seeking to act outside his/her authorization from UNM2000 EMS Client.

3.1.2 Threats

Threats to the TOE are defined as below:

T.Confidentiality	TA.ACCESS_OTE is able to read A.OTE_communication that he is not allowed to read.
T.Integrity	TA.ACCESS_OTE is able to modify A.OTE_communication that he is not allowed to modify.
T.Physical_attack	TA.PHYSICAL gains physical access to the A.OTE_communication and is able to violate Confidentiality and integrity of A.Security parameter and A.OTE_communication.
T.Unauthorised	TA.ROGUE_USER performs actions on the A.Security_parameter that he is not authorized to do.

T.Authorised	TA.ROGUE_USER performs actions on the A.Security_parameter, but it cannot be proven.

3.2 Organizational Security Policies

Security policies to be fulfilled by the TOE are defined as below:

P.FLEXIBLE_MANAGEMENT The TOE must be able to support:

A role-based authorization framework with predefined and customizable roles, to manage the TOE itself.

Manage authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP-address and time of login.

Review logging and auditing of events regularly.

3.3 Assumptions

Assumptions for the IT and non-IT environment and intended usage are defined as below:

A.TRUSTED_NETWORK	It is assumed that the intranet connecting UNM 2000 EMS Server, and EMS Client is trusted and managed with firewall policy. On the other hand the connection between UNM 2000 EMS Server and the OTEs is considered secure and trustful since the WDM/OTN/POTN/DCI protocols are used.
A.TIME_SYNC	It is also assumed that the UNM2000 EMS server underlying Windows Server 2012, which supply time sources are trusted and will not be used to attack the TOE.
A.NO_GENERAL_PURPOSE	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 Security Objectives

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

The Security Objectives for the TOE, describing what the TOE will do to address the threats

The Security Objectives for the Operational Environment, describing what other entities must do to address the threats

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in section 8.1 of this Security Target.

4.1 Security Objectives for the TOE

TOE security objectives are defined as below:

O. Access The TOE shall ensure that OTEs can:

Only send data across pre-defined traffic rules to certain other OTE.

Only receive data across pre-defined traffic rules from other OTE.

Is not able to modify the signal of OTE after the traffic rules was defined.

O.Authorise The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage WDM/OTN/POTN/DCI connecting status from OTE, and manage the role policy. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.

O.Authenticate The TOE shall support a flexible authentication framework for UNM2000 EMS server, allowing accept/reject users from UNM2000 EMS Client

based on: username/password and a configurable subset of IP address and time of login, for verifying if the user's identification was permitted by configured conditions.

O.Auditing The TOE shall support flexible logging and auditing of events. UNM2000 EMS client's user met role policy can access different kinds of log file by UNM 2000 EMS server, which includes monitoring OTEs resource, user behaviour from UNM2000 EMS client, and alerting on suspicious behaviour from UNM 2000 EMS server and OTEs.

O. Manage The TOE provides the management configuration for following items:

Traffic rules of OTEs

Authentication of UNM 2000 EMS Client user

Authorization of access right to UNM 2000 EMS Server

Restriction on user accounts and sessions between UNM 2000 EMS Client to UNM2000 EMS Server

4.2 Security Objectives for the Environment

Security objectives for the Environment (covers objectives for the IT environment and non IT-environment) are defined as below:

OE.SERVER_SECURITY The customer shall ensure that the UNM2000 EMS Server and the OTEs shall be protected from physical intrusion or attacks.

OE.CLIENT_SECURITY The customer shall ensure that only management workstations can host UNM2000 EMS Client, which should be protected from attackers to subsequently:

Disclose passwords or other sensitive information

Hijack the client

OE.TRUST&TRAIN_USERS The customer shall ensure that only assigned appropriately personnel that are sufficiently trustworthy and sufficiently trained to fulfil role policy of TOE.

OE.TIME The underlying O.S. of UNM 2000 EMS Server support clock synchronization.

OE.TRUSTED_NETWORKS The customer shall ensure that:

The connection of intranet should be authorized via pre-defined VPN and firewall policy, so EMS client and UNM2000 EMS server are configured trustful.

The connection between UNM2000 EMS server and the OTEs are performed via VPN using the WDM/OTN/POTN/DCI protocols, therefore, it is considered secure and trustful.

OE.NO_GENERAL_PURPOSE 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. Therefore, users without the administrator rights can not install 3rd party software.

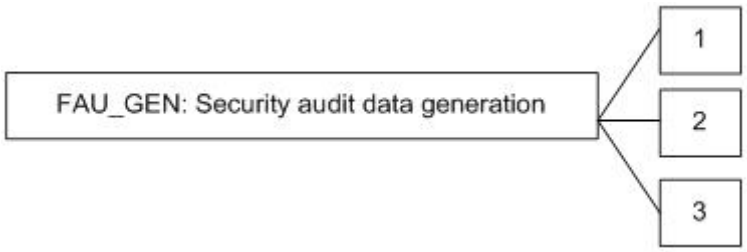
5 Extended Component Definition

FAU_GEN.3 Simplified audit data generation

Family behaviour

This Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

Component levelling



FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

FAU_GEN.3 Add or delete types of events to be logged in the security log.

Management: FAU_GEN.1, FAU_GEN.2, FAU_GEN.3

There are no management activities foreseen.

Audit: FAU_GEN.1, FAU_GEN.2, FAU_GEN.3

There are no auditable events foreseen.

FAU_GEN.3 Simplified audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events: [assignment: *defined auditable events*].

FAU_GEN.3.2 The TSF shall record within each audit record: Date and time of the event, [assignment: *other information about the event*].

6 IT Security Requirements

6.1 Security Functional Requirements

This chapter defines the TOE security functional requirements. A list of the security functional requirements is provided in Table 7. The full text of the security functional requirements is contained below.

The following notational conventions are used in the requirements. Operations are indicated in **bold**, except refinements, which are indicated in ***bold italic***. In general refinements were applied to clarify requirements and/or make them more readable. Iterations were indicated by adding three letters to the component name

Table 7 - TOE security functional requirements

Class	Functional requirement	Title
Access	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification & Authentication	FIA_UID.2	User identification before any action
	FIA_UAU.2	User authentication before any action
	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FTA_SSL.3	TSF-initiated termination
	FTA_MCS.1	Basic limitation on multiple concurrent sessions
Roles & Authorisation	FMT_SMR.1	Security roles
	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
Logging &	FAU_GEN.3	Audit data generation

Class	Functional requirement	Title
Auditing	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
Management	FMT_SMF.1	Specification of Management Functions
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
Protection of the TSF	FPT_STM.1	Time stamps

6.1.1 Access

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [**Traffic Policy**] on [

Ports (any physical Port on OTEs) which receive, send, and modify OTEs traffic.

Services (on Network) which receive, send, and modify security parameters.

]

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [**Traffic Policy**] based on the following types of subject and information security attributes: [

Subjects:

(1) Other network element sending data packages to the OTE. Attributes: source IP, source port, service.

Information:

(1) Data packages from other network elements. Attributes: destination port (physical and logical), network service.

]

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

The OTE ACCEPT data information from other network elements if the configurable rule is explicitly set to ALLOW based on source IP, source port, destination IP, destination port and WDM/OTN/POTN/DCI Signal

FDP_IFF.1.3 The TSF shall enforce the [**additional information flow control SFP rules: OTEs are in the default wavelength**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**none**]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**none**]

6.1.2 Identification & Authentication

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each ***EMS*** user to be successfully identified

by username (in all cases), and

by IP-address (if so configured for that user), and

the user is allowed to login at this time (if so configured for that user)

before allowing any other TSF-mediated actions on behalf of that user

FIA_UAU.2 User authentication before any action

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [**an administrator configurable positive integer within** [**1-99**]] unsuccessful authentication attempts occur related to [**user login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**met**], the TSF shall [

lock the user account until unlocked by the administrator, or

lock the user account until an administrator configurable positive integer within 1-1440 of minutes have passed, if the account has not been set to permanent locking.

]

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

At least 8 characters including three of the four types: number, small letter, capital letter, other characters

cannot contain black spaces

cannot be the username in reverse order or a common dictionary word

can be configured to expire after a configurable amount of time < 999 days

can be configured to be different from the previous 5 or more passwords when changed

]

Application note: the secrets are the user passwords.

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [

configurable period of inactivity more than 30 minutes

when the allowed work time (if so configured for that user) expires

]

FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**1**] session per user.

6.1.3 Roles &Authorisation

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:[

Administrators

Security Administrator Group

Subdomain Security Administrator Group

Ordinary User Group

Operator Group

Maintainer Group

Inspector Group

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

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**Role Policy**] on [

Subjects:

(1)EMS Client Users

Objects:

(1)EMS Server Resources

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application note:

Operations are:

R=Read

D=Delete

C=Create

M=Modify

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [**Role Policy**] to objects based on the following: [

Subjects:

(1)EMS Client Users. Attribute: user role

Objects:

(1)EMS Server Resources. Attribute: none

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a client operation user can be performed upon a server resource as long as the client user role allows performing such actions upon the object and the group that the user belongs has the right to carry out operations over the object category from the particular object.**]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**The users from the administrator group has access to all the**

operations over all the object].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**The users from inspector group has no access to any operations over the objects**].

6.1.4 Logging & Auditing

FAU_GEN.3 Audit data generation

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events: [

authentication success/failure

user account is unlocked

user account is enabled

user account is disabled

events that are set to auditable by an Administrator

]

FAU_GEN.3.2 The TSF shall record within each audit record: [

Date and time of the event,

User name

Type of event

Detailed Information

]

Application note: The TOE maintains 3 separate logs: (1) A security log for authentication events, (2) An operation log for FMT_SMF.1: operations performed by users and (3) A system log for EMS server action record.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**Administrator and suitably customized roles**] with the capability to read [**auditable events**] from the audit records.

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

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorized modifications to the stored audit records in the audit trail.

6.1.5 Protection of the TSF

FPT_STM.1 Reliable time stamps

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

6.1.6 Management

FMT_SMF.1 Specification of Management Functions

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

Table 9 – Management functions

Category	Management function	Related to SFR
OTE	**Manage the Traffic Policy Rules**	**FDP_IFF.1**
EMS	**Set whether a user can only login from certain IP addresses, and if so, which IP addresses**	**FIA_UID.2**
EMS	**Set the time that a user may remain logged in while inactive**	**FTA_SSL.3**
EMS	**Set whether a user is only allowed to work at certain times, and if so, at which times**	**FTA_SSL.3**

Category	Management function	Related to SFR
EMS	**Set the number of allowed unsuccessful authentication attempts**	**FIA_AFL.1**
EMS	**Set the number of hours that an account remains locked**	**FIA_AFL.1**
EMS	**Set whether a user account should be:** o **unlockable, or** o **locked (either permanently or temporarily)** **when it exceeds the number of allowed consecutive unsuccessful authentication attempts**	**FIA_AFL.1**
EMS	**Unlock a user account**	**FIA_AFL.1**
EMS	**Set whether a user password expires after a certain time, and if so, after how long**	**FIA_SOS.1**
EMS	**Set whether the new password of a user must be different from the last n passwords when the password is changed by the user and configure n**	**FIA_SOS.1**
EMS	**Set the maximum number of concurrent sessions for the same user**	**FTA_MCS.1**
EMS	**Create, edit and delete customized roles**	**FMT_SMR.1**
EMS	**Add or remove roles to/from users**	**FMT_SMR.1**
EMS	**Add types of events to be logged in the security log**	**FAU_GEN.3.1**
EMS	**Create, edit and delete user accounts**	**FDP_ACC.2** **FDP_ACF.1**
EMS	**Disable/enable user accounts**	**FDP_ACC.2** **FDP_ACF.1**

Category	Management function	Related to SFR
EMS	**Lock/unlock roles**	**FDP_ACC.2** **FDP_ACF.1**
OTE	**Adding, deleting and modifying rules in the Taffic Policy**	**FDP_IFC.1,** **FDP_IFF.1**

]

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**Role Policy**] to restrict the ability to [**change_default, query, modify, delete**] the security attributes [**user role, access rights to operations]** to [**Administrators**].

FMT_MSA.3 Static attribute initialisation

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

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

6.2 Security Assurance Requirements

The security assurance requirements for the TOE are the assurance components of evaluation assurance level 2 (EAL 2) augmented ALC_FLR.2. They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 9.

Table 10 – Security Assurance Requirements

Assurance class	Assurance component (Identifier & Name)
Development(ADV)	ADV_ARC.1 Security architecture description

Assurance class	Assurance component (Identifier & Name)	
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw reporting procedures**
Security target evaluation (ASE)	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)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment (AVA)	AVA_VAN.2	Vulnerability analysis

6.3 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL2+ALC_FLR.2. The reasons for this choice are that:

EAL 2 is deemed to provide a good balance between assurance and costs and is in line with FiberHome customer requirements.

ALC_FLR.2 provides assurance that FiberHome has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with FiberHome customer requirements.

The refinements are derived from FiberHome customer requirements as well.

7 TOE Summary Specification

Access control:

OTE transport data of WDM/OTN/POTN/DCI connecting status, in such a way that:

Only the intended recipients from UNM2000 EMS server are able to read OTE signal.

Nobody can modify the signals of OTE, which was monitored by UNM2000 EMS server.

- Nobody can modify the signals

FDP_IFC.1, FDP_IFF.1

The TOE enforce OTE's data transport by Traffic rule:

OTEs' Ports are physically isolated from each other, and can only talk to each other through a switch in the TOE with pre-defined traffic rule.

OTEs' signal cannot be modified with pre-defined traffic rule.

Authentication:

The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users from UNM2000 EMS client based on: username/password and a configurable subset of IP address and time of login.

General:

TOE provides GUI authentication interface, which provide security control with:

FIA_UID.2, FIA_UAU.2, FIA_AFL.1

Whenever a user need to access UNM2000 EMS Server, the user needs to be granted access right by login UNM2000 EMS client,

Authorization:
The TOE supports a flexible role-based authorization framework with predefined and customizable roles for management. These roles can use the UNM2000 EMS server to manage OTEs.

FMT_SMR.1, FDP_ACC.2, FDP_ACF.1,

The TOE allows management of the telecommunications network by different users. The TOE can be configured to give each user precisely the access to the resources of the telecommunication network that user needs to do his job. To assist in this, the TOE has a number of pre-defined roles:

Administrators: This user group has the management domain over assembly of objects and operation authorities over assembly of application operations.

Security Administrator Group: This user group has the operation authorities related to the security management, including user management and online user management.

Subdomain Security Administrator Group: The Subdomain Security Administrator Group, created by the security administrator and with its management domain assigned by the security administrator, only has the security management authority, which cannot be modified.

Ordinary User Group: The Ordinary User Group is created by the security administrator (user in the Security Administrator Group) or subdomain security administrator (user in the Subdomain Security Administrator Group). The management domain and operation authority of the users in this group are assigned by the security administrator or subdomain security administrator (When a subdomain security administrator assigns authority to other users, he cannot assign authority of Administrators group or Security Administrator Group).

Operator Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application operators by default. The member in this group not only has the operation authority of the inspector group, but also can

configure, create and delete data.

Maintainer Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application maintainers by default. The member in this group not only has the authority of inspector group and operator group, but also can configure and download the EMS and device function related data.

Inspector Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application inspectors by default. The member in this group can only view, query, count, and export data rather than configure or create data.

and can assign these roles to specific users.

Audit:

UNM2000 EMS server supports flexible logging and auditing of events.

Records in log files can provide the following uses: monitoring system resources; auditing user behaviour; alerting on suspicious behaviour.

FAU_GEN.3, FAU_SAR.1, FAU_STG.1, FPT_STM.1

The TOE maintains a security log for authentication events, and supports different log view criteria according to role policy.

Management:

The TOE manages traffic rules, authentication, authorization, user accounts and sessions.

FMT_SMF.1

The TOE allows the Administrator to configure (for each user), what/how/when user was allowed to log-in:

FMT_MSA.1, FMT_MSA.3

The TOE allows specifying secure values to the attributes used in the access control policy, for enabling user roles to access different management operations.

FTA_MCS.1, FTA_SSL.3

Session Limitation, conditional block for advanced account management.

FIA_SOS.1

Support password policy by request.

8 Rationale

8.1 Rationale for Security Objectives

Table 11 – Rationale for security objectives (1)

Security objectives / Threat/OSP/ Assumption	O.AUTHORISE	O.AUTHENTICATE	O. ACCESS	O.AUDITING	O.MANAGE	OE.SERVER_SECURITY	OE.CLIENT_SECURITY	OE.TRUST&TRAIN_USERS	OE.TIME	OE.TRUSTED_NETWORKS	OE.NO_GENERAL_PURPOSE
T. Confidentiality			X								
T.Integrity			X								
T.Physical_attack		X			X	X		X			
T.Unauthorised	X	X			X		X	X			
T.Authorised				X				X			
P.FLEXIBLE_MANAGEMENT				X	X				X		
A.TRUSTED_NETWORK										X	
A.TIME_SYNC									X		
A.NO_GENERAL_PURPOSE											X

Table 12 – Rationale for security objectives (2)

Assumptions/OSPs/Threats	Objectives
T.Confidentiality TA.ACCESS_OTE is able to read A.OTE_communication that he is not allowed to read.	This threat is countered by O.ACCESS, which ensure traffic rules on OTEs.
T.Integrity TA.ACCESS_OTE is able to modify A.OTE_communication that he is not allowed to modify	This threat is countered by the third bullet of O.ACCESS, which ensure traffic rules on OTEs.
T.Physical_attack TA.PHYSICAL gains physical access to the A.OTE_communication and is able to violate Confidentiality and integrity of A.Security parameter and A.OTE_communication.	This threat is countered by: O.AUTHENTICATE, EMS server can verify user's identification and IP address. O.MANAGE, provides management configuration item of OTEs' traffic rule and EMS server's authorization. OE.SERVER_SECURITY, Access to the EMS server and OTEs should be managed by customer. OE.TRUST&TRAIN_USERS, requiring that the administrator's role with privilege should be trusted and trained by customer.
T.Unauthorised TA.ROGUE_USER performs actions on the A Security parameter that he is not authorized to do.	This threat is countered by four security objectives: O.AUTHORISE, providing role-based management for granting access right. O.AUTHENTICATE EMS server can verify user's identification and IP address. O.MANAGE provides management configuration

Assumptions/OSPs/Threats	Objectives
	item of EMS server's authorization. OE.TRUST&TRAIN_USERS, requiring that the user's role with privilege should be trusted and trained by customer. OE.CLIENT_SECURITY, the EMS Client should be protected by customer for preventing sensitive information leak, Hijack, and min-in-the-middle attack.
T.Authorised TA.ROGUE_USER performs actions on the A.Security_parameter, but it cannot be proven.	This threat is countered by: O.AUDITING will ensure that the actions of the user can be traced back to him. OE.TIME support the proving evidence on EMS server.
P.FLEXIBLE_MANAGEMENT The TOE must be able to support: A role-based authorization framework with predefined and customizable roles, to manage the TOE itself. Manage authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP-address and time of login. Review logging and auditing of events regularly.	This OSP is primarily implemented by the combination of three security objectives O.MANAGE provides management configuration item on role policy and authorization. O.AUDITING will ensure that the actions of the user can be traced back to him. OE.TIME support the proving evidence on EMS server.
A.TRUSTED_NETWORK	This assumption is upheld by

Assumptions/OSPs/Threats	Objectives
It is assumed that the intranet connecting UNM 2000 EMS Server, and EMS Client is trusted and managed with firewall policy. On the other hand the connection between UNM 2000 EMS Server and the OTEs is considered secure and trustful since the WDM/OTN/POTN/DCI network protocols are used.	OE.TRUSTED_NETWORK, connection of intranet should managed and authorized by customer. On the other hand, UNM2000 EMS server and OTEs connection are performed via VPN using the WDM/OTN/POTN/DCI network protocols, therefore, it is considered secure and trustful.
A.TIME_SYNC It is also assumed that the UNM2000 EMS server underlying Windows Server 2012, which supply time sources are trusted and will not be used to attack the TOE.	This assumption is upheld by OE.TIME support the clock synchronization.
A.NO_GENERAL_PURPOSE 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.	This assumption is upheld by OE.NO_GENERAL_PURPOSE support the clock synchronization.

8.2 Security Functional Requirements Rationale

Table 13 – Rationale for SFRs (1)

Security objectives / Security functional requirements	O. ACCESS	O.AUTHORISE	O.AUTHENTICATE	O.AUDITING	O.MANAGE
FDP_IFC.1	X				
FDP_IFF.1	X				
FIA_UID.2			X		
FIA_UAU.2			X		
FIA_AFL.1			X		
FIA_SOS.1			X		X
FTA_SSL.3			X		X
FTA_MCS.1			X		X
FMT_SMR.1		X			
FDP_ACC.2		X			
FDP_ACF.1		X			
FAU_GEN.3				X	
FPT_STM.1				X	
FAU_SAR.1				X	
FAU_STG.1				X	

Security objectives / Security functional requirements	O. ACCESS	O.AUTHORISE	O.AUTHENTICATE	O.AUDITING	O.MANAGE
FMT_SMF.1	**X**	**X**	**X**	**X**	**X**
FMT_MSA.1					**X**
FMT_MSA.3					**X**

Table 14 - Rationale for SFRs (2)

Security objectives	SFRs addressing the security objectives
O. Access The TOE shall ensure that client-side equipment can: Only send data across the network to certain other client-side equipment Only receive data across the network from that client-side equipment Is not able to modify data that is not created by it or sent to it.	This objective is met by FDP_IFF.1 and FDP_IFC.1 specifying that there are rules regulating the access and FMT_SMF.1 allowing management of these rules.
O.Authorise The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the WDM/OTN/POTN/DCI	This objective is met by: FMT_SMR.1 stating the predefined and customizable roles. FDP_ACC.2 and FDP_ACF.1 defining a Role

Security objectives	SFRs addressing the security objectives
network and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.	Policy, which states how the various roles manage the network and the TOE. These also state that only roles can perform actions(operations on resources) and therefore users can only do this when they have the correct role FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible, role-based authorization framework.
O.Authenticate The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: Username / password and a configurable subset of IP-address and time of login.	This objective is met by: FIA_UID.2 stating that identification will be done by username, password, IP/MAC-address, login time FIA_UAU.2 stating that users must be authenticated FIA_SOS.1 stating that passwords must have a minimum quality FIA_AFL.1 stating what happens when authentication fails repeatedly FTA_SSL.3 logging users off when they are no longer allowed to work or when their role is locked FTA_MCS.1 preventing a user of having too many sessions or all users together having too many sessions FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible

Security objectives	SFRs addressing the security objectives
	authentication framework.
O.Auditing The TOE shall support flexible logging and auditing of events.	This objective is met by: FAU_GEN.3 showing which events are logged FAU_SAR.1 showing that the logged events can be audited and by whom FAU_STG.1 showing how the audit logs are protected FMT_SMF.1 configuring all of the above Together, these SFRs support a flexible logging and auditing framework.
O.Manage The TOE provides the management configuration for following items: Traffic rules of OTEs Authentication of UNM 2000 EMS Client user Authorization of access right to UNM 2000 EMS Server Restriction on user accounts and sessions between UNM 2000 EMS Client to UNM2000 EMS Server	This objective is met by: FMT_SMF.1 allows administrator to configure the user's privilege. FTA_MCS.1 provides conditional block to account. FTA_SSL.3 provides session limitation for account management. FIA_SOS.1 support customized password policy. FMT_MSA.1 allows managing the security attributes of the access control policy. FMT_MSA.3 allows managing the security attributes of the access control policy.

8.2.1 Dependencies Rationale

Table 12 - Rationale for dependencies of security functional requirements

SFR	Dependencies
FAU_GEN.3	FPT_STM.1: met in the environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FAU_STG.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FDP_ACC.2	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met by FDP_ACC.2 FMT_MSA.3: met.
FDP_IFC.1	FDP_IFF.1: met
FDP_IFF.1	FDP_IFC.1: met FMT_MSA.3: unnecessary, since the information control policy attributes cannot be managed.
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_SOS.1	_
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	_
FMT_SMF.1	_
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FMT_MSA.1	FDP_ACC.1: met by FDP_ACC.2 FMT_SMR.1: met by FMT_SMR.1

SFR	Dependencies
	FMT_SMF.1: met by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1: met by FMT_MSA.1 FMT_SMR.1: met by FMT_SMR.1
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FTA_SSL.3	_

9 Appendix

9.1 Acronyms

EMS	Element Management System
NMS	Network Management System
DCI	Data Center Interconnection
ONT	Optical Network Terminal
OTE	Optical Transport Equipment
UNM	Unified Network Management
POTN	Packet Enhanced Optical Transport Network
WDM	Wave Division Multiplexing

9.2 References

[CC] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, dated April 2017, Version 3.1, Revision 5 CCMB- 2017-04-001/2/3

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated April 2017, Version 3.1, Revision 5 CCMB- 2017-04-001/2/3

Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated April 2017, Version 3.1, Revision 5 CCMB- 2017-04-001/2/3

[CEM] *Common Evaluation Methodology for Information Technology Security Evaluation*, dated April 2017, Version 3.1, Revision 5 CCMB-2017-04-001/2/3