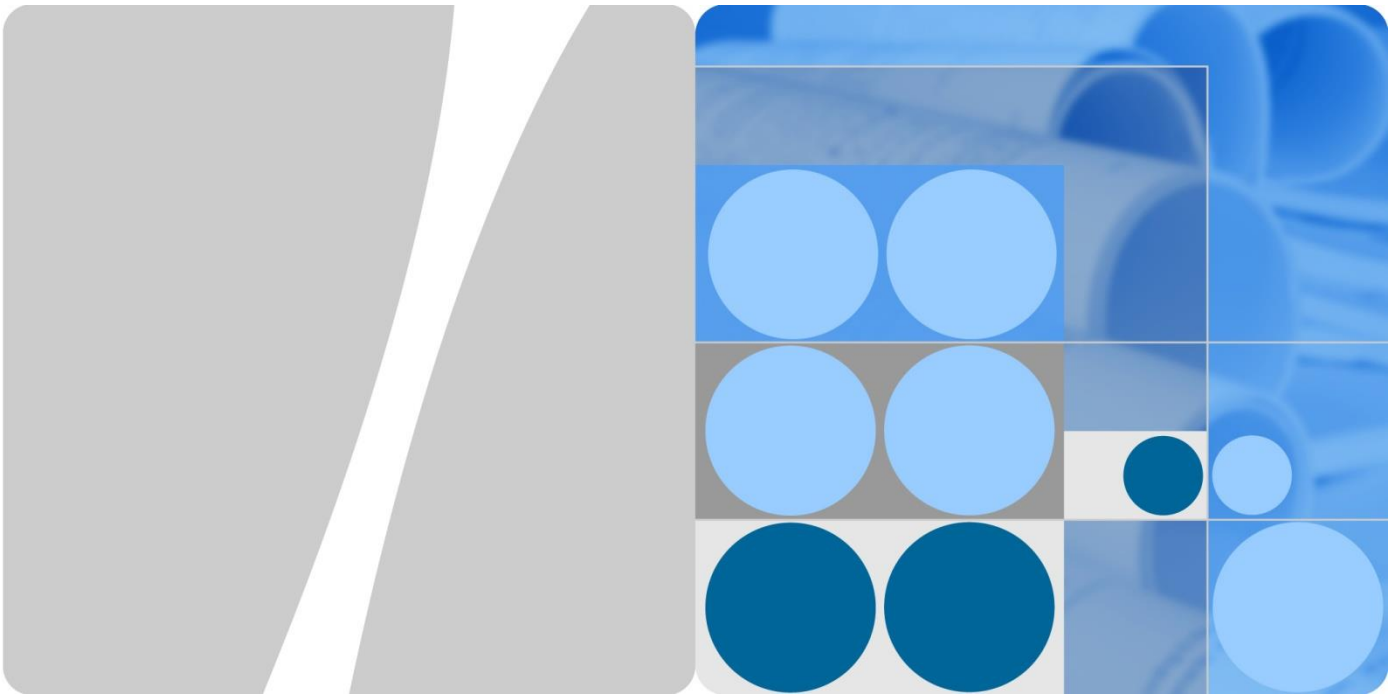


USP Running on Huawei Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L) V100R13C00

Security Target

Issue 1.7

Date 2014-12-12

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

Figures

Tables

1 Introduction

This Security Target (ST) is for the security evaluation of universal software platform (USP) running on Huawei transmission equipment series. Huawei transmission equipment series include OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L.

1.1 ST Identification

This ST is uniquely identified as below:

Title: USP Running on Huawei Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L) V100R013C00

Version: V1.7

Author: Huawei Technologies Co., Ltd.

Publication date: 2014-12-12

1.2 TOE Identification

Name: USP Running on Huawei Transmission Equipment Series (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L)

Version: USP V100R013C00, OptiX OSN 1800 V100R005C10SPC210，OptiX OSN 3800 V100R009C00SPC300，OptiX OSN 3800A V100R009C00SPC300，OptiX OSN 6800 V100R009C00SPC300，OptiX OSN 6800A V100R009C00SPC300，OptiX OSN 8800 V100R009C00SPC300， OptiX OSN 9600 V100R001C20SPC300，OptiX OSN 9800 V100R001C20SPC300， OptiX OSN 500 V100R007C20SPH203，OptiX OSN 550 V100R007C20SPH203，OptiX OSN 580 V100R007C20SPH203，OptiX OSN 1500 V200R013C20SPH303， OptiX OSN 3500 V200R013C20SPH303，OptiX OSN 7500 V200R013C20SPH303，OptiX OSN 7500II V200R013C20SPH303，OptiX RTN 360

V100R001C00SPH101，OptiX RTN 380 V100R002C00SPH201， OptiX RTN 905 V100R007C00SPH102，OptiX RTN 950 V100R007C00SPH102，OptiX RTN 950A V100R007C00SPH102，OptiX RTN 980 V100R007C00SPH102，OptiX RTN 980L V100R007C00SPH102

Developer: Huawei Technologies Co., Ltd.

TOE release date: 2014-11-12

VRC versions are defined as follows:

- V version is the version of the software or hardware platform that a product bases.
- R version is released for customer at a specific time. It is a collection of features that is embodied in the form of a product.
- C version is the customized version developed based on the R version to fast meet customer demands.

The TOE can be a WDM/OTN product (see Table 1-1), MSTP product (see Table 1-2**)**,or RTN product (see Table 1-3).USP is platform software running on these product.

OptiX OSN 8800/1800/9800 series are three Huawei WDM product families that base on the USP platform. OptiX OSN 1800 series are used at the access layer, OptiX OSN 8800 series are used at the backbone layer, and OptiX OSN 9800 series are used at the core layer of WDM networks.

Table 1-1 lists the available chassis in each product family.

Table 1-1 Chassis of WDM/OTN product series

Chassis	Product Version	USP Software Version
OptiX OSN 1800 I	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 II	V100R005C10SPC210	USPV100R013C00
OptiX OSN 1800 V	V100R005C10SPC210	USPV100R013C00
OptiX OSN 8800 T64	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T32	V100R009C00SPC300	USPV100R013C00
OptiX OSN 8800 T16	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 6800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800	V100R009C00SPC300	USPV100R013C00
OptiX OSN 3800A	V100R009C00SPC300	USPV100R013C00
OptiX OSN 9800 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9800 U32	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U64	V100R001C20SPC300	USPV100R013C00
OptiX OSN 9600 U32	V100R001C20SPC300	USPV100R013C00

OptiX OSN 5X0/3500 series are two Huawei MSTP product families that base on the USP platform. They are widely used at the access layer, convergence layer and backbone layer of MSTP networks.

Table 1-2 lists the available chassis in each product family.

Table 1-2 Chassis of MSTP product series

Chassis	Product Version	USP Software Version
OptiX OSN 500	V100R007C20SPH203	USPV100R013C00
OptiX OSN 550	V100R007C20SPH203	USPV100R013C00
OptiX OSN 580	V100R007C20SPH203	USPV100R013C00
OptiX OSN 1500A	V200R013C20SPH303	USPV100R013C00
OptiX OSN 1500B	V200R013C20SPH303	USPV100R013C00
OptiX OSN 3500	V200R013C20SPH303	USPV100R013C00
OptiX OSN 7500	V200R013C20SPH303	USPV100R013C00
OptiX OSN 7500 II	V200R013C20SPH303	USPV100R013C00

The RTN transmission system is a microwave radio system that bases on the USP platform. Providing transmission from the access layer to the backbone layer, the product series support carrier-class Ethernet features for supporting the mobile backhaul evolution from GSM, UMTS, to LTE.

Table 1-3 lists the available chassis in RTN product series.

Table 1-3 Chassis of RTN product series

Chassis	Product Version	USP Software Version
OptiX RTN 380	V100R002C00SPH201	USPV100R013C00
OptiX RTN 360	V100R001C00SPH101	USPV100R013C00
OptiX RTN 9051C	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052A	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9051E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 9052E	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950	V100R007C00SPH102	USPV100R013C00
OptiX RTN 950A	V100R007C00SPH102	USPV100R013C00

Chassis	Product Version	USP Software Version
OptiX RTN 980	V100R007C00SPH102	USPV100R013C00
OptiX RTN 980L	V100R007C00SPH102	USPV100R013C00

1.3 TOE Overview

1.3.1 TOE Type

The TOE is the Optical Transmission Equipment (OptiX OSN 1800/3800/3800A/6800/6800A/8800/9600/9800, OptiX OSN 500/550/580, OptiX OSN 1500(A/B)/3500/7500/7500 II, and OptiX RTN 360/380/905(1A/1C/1E/2A/2E)/950/950A/980/980L),which consists of the hardware and the software.

The hardware is composed of cabinet, chassis, power supply and single board. Cabinet mainly provides to support and power supply interface sub frame installation.

Power supply to the cabinet sub frame. The sub frame provides the main backplane, single board slot and signal input and output interface of the single board.

Single board is the transmission equipment business processing and management of the core unit. Each single board to complete different business functions, including signal amplification and regeneration, business multiplexing / demultiplexing, clock signal processing, save the service configuration data and recovery etc.. Single board different through the communication interface between single boards of management and control of information transfer and interaction. Each single board is an independent embedded system, USP as the management software to run on the board.

Transmission network hardware provide management interfaces and service interfaces, the interface of different types and quantities of equipment type support has the difference.

The USP is the software core of the transmission equipment. It is the software platform for managing and running communication networking functionalities.

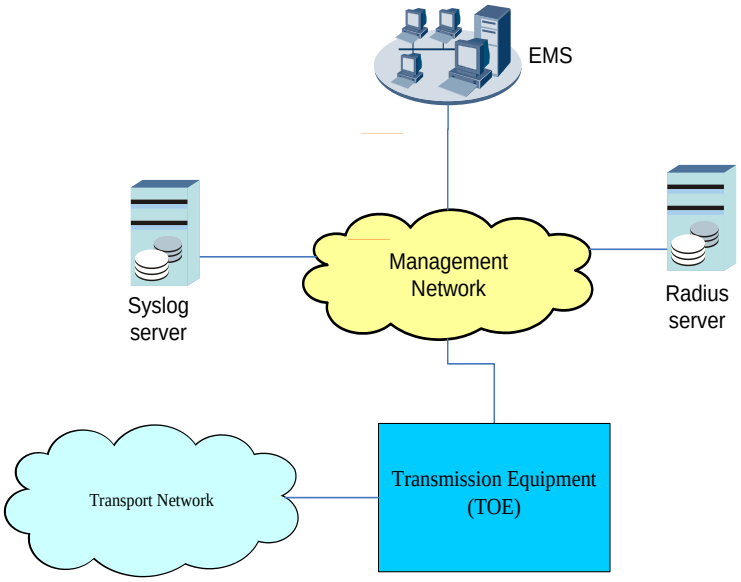
USP provides service configuration and product software management features.

USP provides extensive security features. These features include different interfaces for various access modes, enforced authentication prior to establishment of administrative sessions with the TOE, and auditing of security-related management activities, as well as flexible logging and auditing of events.

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Authentication
2. Authorization
3. Auditing
4. Communication Security
5. Access Control

These features are described in more detail in the subsections below.



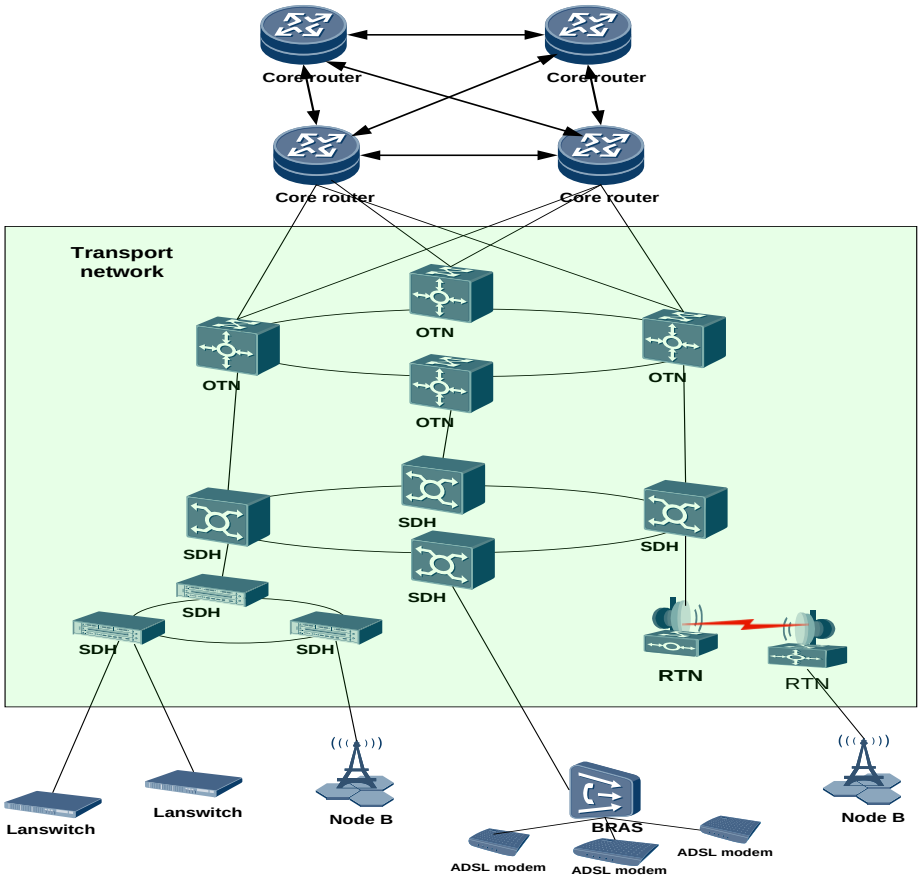
1.3.2 Non-TOE Hardware and Software

The TOE requires non-TOE hardware and software, including the EMS (client and server), Syslog server, and RADIUS server, as shown in the preceding figure.

1.3.3 TOE in Network Environments

Transport networks (including SDH, RTN, and WDM/OTN networks) transparently transmit client services from one place to another. For example, as shown in Figure 1-1, Ethernet services are transmitted from LAN switch to SDH equipment, then to OTN equipment, and finally to core routers for routing. During the transmission, transmission equipment encapsulates client services into signals of certain rates, performs error control, and monitors the quality of the signals. To achieve transparent transmission, the transmission equipment does not process client services transmitted from other equipment.

Figure 1-1 Position of the transport network on the entire communication network



Located at the transport layer of a communication network, Huawei transmission equipment provides large-capacity and high-reliability transparent transmission tunnels, and is almost invisible to end users. The transmission tunnels are not prone to external attacks.

The transmission equipment provides high-end networking capacities for telecom and enterprise core networks, which consists of both hardware and software. The transmission equipment processes three categories of data: O&M data, control plane data, and service data. The preceding data is transmitted over independent logical and physical paths and does not affect each other.

1.4 TOE Description

1.4.1 Physical Scope

1.4.1.1 Physical Scope of WDM/OTN product series

WDM/OTN product series include OptiX OSN 1800 series, OptiX OSN 8800 series and OptiX OSN 9800 series.

1.4.1.1.1 Physical Scope of OptiX OSN 1800 series

OptiX OSN 1800 I V100R005C10SPC210

Hardware	OptiX OSN 1800 I
Software	OptiX OSN 1800 I V100R005C10SPC210
Guidance	OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01
OptiX OSN 1800 II V100R005C10SPC210	
Hardware	OptiX OSN 1800 II
Software	OptiX OSN 1800 II V100R005C10SPC210
Guidance	OSN 1800 I/II Compact Multi-Service Edge Optical Transport Platform V100R005C10 Product Documentation-01
OptiX OSN 1800 V V100R005C10SPC210	
Hardware	OptiX OSN 1800 V
Software	OptiX OSN 1800 V V100R005C10SPC210
Guidance	OSN 1800 V Packet Enhanced V100R005C10 Deploying Your Network 01 OSN 1800 V Packet Enhanced V100R005C10 Installing, Operating and Maintaining Your Network (For Field Engineer) 01 OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 1st Line Engineer) 01 OSN 1800 V Packet Enhanced V100R005C10 Operating and Maintaining Your Network (For 2nd Line Engineer) 01 OSN 1800 V Packet Enhanced V100R005C10 Planning Your Network 01

1.4.1.1.2 Physical Scope of OptiX OSN 8800 series

OptiX OSN 8800 series is a product family, including the following chassis:

- OptiX OSN 8800 T16
- OptiX OSN 8800 T32
- OptiX OSN 8800 T64
- OptiX OSN 3800
- OptiX OSN 6800
- OptiX OSN 3800A
- OptiX OSN 6800A

OptiX OSN 8800 V100R009C00SPC300	
Hardware	OptiX OSN 8800 T16
Software	OptiX OSN 8800 V100R009C00SPC300
Guidance	OptiX OSN 8800 V100R009C00 Product Documentation 01
OptiX OSN 8800 V100R009C00SPC300	
Hardware	OptiX OSN 8800 T32
Software	OptiX OSN 8800 V100R009C00SPC300
Guidance	OptiX OSN 8800 V100R009C00 Product Documentation 01
OptiX OSN 8800 V100R009C00SPC300	
Hardware	OptiX OSN 8800 T64
Software	OptiX OSN 8800 V100R009C00SPC300
Guidance	OptiX OSN 8800 V100R009C00 Product Documentation 01
OptiX OSN 3800 V100R009C00SPC300	

Hardware	OptiX OSN 3800
Software	OptiX OSN 3800 V100R009C00SPC300
Guidance	OptiX OSN 3800 V100R009C00 Product Documentation 01
OptiX OSN 6800 V100R009C00SPC300	
Hardware	OptiX OSN 6800
Software	OptiX OSN 6800 V100R009C00SPC300
Guidance	OptiX OSN 6800 V100R009C00 Product Documentation 01
OptiX OSN 3800A V100R009C00SPC300	
Hardware	OptiX OSN 3800
Software	OptiX OSN 3800A V100R009C00SPC300
Guidance	OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)
OptiX OSN 6800A V100R009C00SPC300	
Hardware	OptiX OSN 6800
Software	OptiX OSN 6800A V100R009C00SPC300
Guidance	OptiX OSN 8800 6800A 3800A V100R008C00 Product Documentation 01(NA)

1.4.1.1.3 Physical Scope of OptiX OSN 9800 series

OptiX OSN 9800 series is a product family, including the following chassis：

- OptiX OSN 9800 U64
- OptiX OSN 9800 U32
- OptiX OSN 9600 U64
- OptiX OSN 9600 U32

OptiX OSN 9800 U64 V100R001C20SPC300	
Hardware	OptiX OSN 9800 U64
Software	OptiX OSN 9800 V100R001C20SPC300
Guidance	OSN 9800 V100R001C20 Planning Your Network 01 OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01 OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01 OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01 OSN 9800 V100R001C20 Deploying Your Network 01
OptiX OSN 9800 U32 V100R001C20SPC300	
Hardware	OptiX OSN 9800 U32
Software	OptiX OSN 9800 V100R001C20SPC300
Guidance	OSN 9800 V100R001C20 Planning Your Network 01 OSN 9800 V100R001C20 Installing, Operating and Maintaining Your Network (For Field Engineer) 01 OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 2nd Line Engineer) 01 OSN 9800 V100R001C20 Operating and Maintaining Your Network (For 1st Line Engineer) 01 OSN 9800 V100R001C20 Deploying Your Network 01
OptiX OSN 9600 U64 V100R001C20SPC300	

Hardware	OptiX OSN 9600 U64
Software	OptiX OSN 9600 V100R001C20SPC300
Guidance	OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01 OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01 OSN 9600 V100R001C20 开局指导 01 OSN 9600 V100R001C20 规划指导 01 OSN 9600 V100R001C20 站点操作指导 01
OptiX OSN 9600 U32 V100R001C20SPC300	
Hardware	OptiX OSN 9600 U32
Software	OptiX OSN 9600 V100R001C20SPC300
Guidance	OSN 9600 V100R001C20 运维指导（网络运维工程师用书）01 OSN 9600 V100R001C20 运维指导（网络监控工程师用书）01 OSN 9600 V100R001C20 开局指导 01 OSN 9600 V100R001C20 规划指导 01 OSN 9600 V100R001C20 站点操作指导 01

1.4.1.2 Physical Scope of OSN series

1.4.1.2.1 Physical Scope of 5x0 series

OptiX OSN 500 V100R007C20SPH203	
Hardware	OptiX OSN 500
Software	OptiX OSN 500 V100R007C20SPH203
Guidance	OSN 500 V100R007C20 Product Description 01(pdf).zip OSN 500 V100R007C20 Hardware Description 01(pdf).zip OptiX OSN 500 Quick Installation Guide 04(pdf).zip OptiX OSN 500 V100R007C20 Security White Paper.doc OptiX OSN 500 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 550 V100R007C20SPH203	
Hardware	OptiX OSN 550
Software	OptiX OSN 550 V100R007C20SPH203
Guidance	OSN 550 V100R007C20 Product Description 01(pdf).zip OSN 550 V100R007C20 Hardware Description 01(pdf).zip OptiX OSN 550 Quick Installation Guide 03(pdf).zip OptiX OSN 550 Quick Installation Guide for Outdoor Cabinets (APM30H&TMC11H) 04(pdf).zip OptiX OSN 550 V100R007C20 Security White Paper.doc OptiX OSN 550 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 580 V100R007C20SPH203	
Hardware	OptiX OSN 580
Software	OptiX OSN 580 V100R007C20SPH203
Guidance	OSN 580 V100R007C20 Product Description 01(pdf).zip OSN 580 V100R007C20 Hardware Description 01(pdf).zip OptiX OSN 580 Quick Installation Guide 02(pdf).zip

	OptiX OSN 580 Quick Installation Guide for Outdoor Cabinets (Mini-shelter) 01(pdf).zip OptiX OSN 580 V100R007C20 Security White Paper.doc OptiX OSN 580 V100R007C20 Security Configuration, Maintenance, and Hardening Manual.doc

1.4.1.2.2 Physical Scope of OSN1500/3500/7500/7500II

OptiX OSN 1500A V200R013C20SPH303	
Hardware	OptiX OSN 1500A
Software	OptiX OSN 1500A V200R013C20SPH303
Guidance	OSN 1500 V200R013C20 Product Description 01 OSN 1500 V200R013C20 Hardware Description 01 OSN 1500 Quick Installation Guide 13 OptiX OSN 1500 V200R013C20 Security White Paper.doc OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 1500B V200R013C20SPH303	
Hardware	OptiX OSN 1500B
Software	OptiX OSN 1500B V200R013C20SPH303
Guidance	OSN 1500 V200R013C20 Product Description 01 OSN 1500 V200R013C20 Hardware Description 01 OSN 1500 Quick Installation Guide 13 OptiX OSN 1500 V200R013C20 Security White Paper.doc OptiX OSN 1500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 3500 V200R013C20SPH303	
Hardware	OptiX OSN 3500
Software	OptiX OSN 3500 V200R013C20SPH303
Guidance	OSN 3500 V200R013C20 Product Description 01 OSN 3500 V200R013C20 Hardware Description 01 OSN 3500 Quick Installation Guide 16 OptiX OSN 3500 V200R013C20 Security White Paper.doc OptiX OSN 3500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 7500 V200R013C20SPH303	
Hardware	OptiX OSN 7500
Software	OptiX OSN 7500 V200R013C20SPH303
Guidance	OSN 7500 V200R013C20 Product Description 01 OSN 7500 V200R013C20 Hardware Description 01 OSN 7500 Quick Installation Guide 16 OptiX OSN 7500 V200R013C20 Security White Paper.doc OptiX OSN 7500 V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc
OptiX OSN 7500 II V200R013C20SPH303	
Hardware	OptiX OSN 7500 II

Software	OptiX OSN 7500 II V200R013C20SPH303
Guidance	OSN 7500 II V200R013C20 Product Description 01 OSN 7500 II V200R013C20 Hardware Description 01 OSN 7500 II Quick Installation Guide 07 OptiX OSN 7500II V200R013C20 Security White Paper.doc OptiX OSN 7500II V200R013C20 Security Configuration, Maintenance, and Hardening Manual.doc

1.4.1.3 Physical Scope of RTN series

1.4.1.3.1 Physical Scope of RTN 300 series

The RTN 300 series IP microwave radio is highly compact fully outdoor microwave. Products include the RTN 360, RTN 380.

OptiX RTN 360 V100R001C00SPH101	
Hardware	RTN 360
Software	OptiX RTN 360 V100R001C00SPH101
Guidance	RTN 360 V100R001C00 Product Documentation
OptiX RTN 380 V100R002C00SPH201	
Hardware	RTN 380
Software	OptiX RTN 380 V100R002C00SPH201
Guidance	RTN 380 V100R002C00 Product Documentation

1.4.1.3.2 Physical Scope of RTN 900 series

The RTN 900 series IP microwave Products include the RTN 905(1A/2A/1C/1E/2E), RTN 950, RTN 950A, RTN 980 and RTN 980L.

OptiX RTN 905 1A&2A V100R007C00SPH102	
Hardware	IDU 905 1A&2A
Software	OptiX RTN 905 1A&2A V100R007C00SPH102
Guidance	RTN 905 1A&2A&1C V100R007C00 Product Documentation
OptiX RTN 905 1C V100R007C00SPH102	
Hardware	IDU 905 1C
Software	OptiX RTN 905 1C V100R007C00SPH102
Guidance	RTN 905 1A&2A&1C V100R007C00 Product Documentation
OptiX RTN 905 1E&2E V100R007C00SPH102	
Hardware	IDU 905 1E&2E
Software	OptiX RTN 905 1E&2E V100R007C00SPH102
Guidance	RTN 905 1E&2E V100R007C00 Product Documentation
OptiX RTN 950 V100R007C00SPH102	
Hardware	IDU 950
Software	OptiX RTN 950 V100R007C00SPH102
Guidance	RTN 950 V100R007C00 Product Documentation
OptiX RTN 950A V100R007C00SPH102	
Hardware	IDU 950A

Software	OptiX RTN 950A V100R007C00SPH102
Guidance	RTN 950A V100R007C00 Product Documentation
OptiX RTN 980 V100R007C00SPH102	
Hardware	IDU 980
Software	OptiX RTN 980 V100R007C00SPH102
Guidance	RTN 980 V100R007C00 Product Documentation
OptiX RTN 980L V100R007C00	
Hardware	IDU 980L
Software	OptiX RTN 980L V100R007C00SPH102
Guidance	RTN 980L V100R007C00 Product Documentation

1.4.1.3.3 Physical scope of the Platform

Software	USP V100R013C00
Guidance	Huawei Transmission Equipment Series Certified Configuration v1.4

1.4.2 Logical Scope

In order to provide high-capacity and high-reliability transparent transmission service, the TOE is logically divided into three independent planes: management plane，control plane and service (or data) plane. The management plane provides OAM (Operation, Administration and Maintenance) functions for the TOE. Only the management plane faces the security threats. The TOE provides several major security features as follows.

1.4.2.1 Authentication

The TOE can authenticate administrative users by user name and password.

USP provides a local authentication scheme, or can optionally enforce authentication decisions obtained from a Radius server in the IT environment.

Authentication is always enforced for virtual terminal sessions via SSL.

1.4.2.2 Authorization

The TOE controls access by the role-based authorization framework with predefined and customizable roles for management. Five hierarchical access role groups are offered and can be assigned to individual user accounts.

Accounts are managed in groups and each group represents a specific authority assigned to the accounts in the group. For example, the accounts of the "administrator" role are authorized to perform all security management and maintenance operations. If an account attempts to perform any unauthorized operation, an error message is displayed and the attempt is logged.

Table 1-4 Groups role of accounts

Group	Rights
Monitoring personnel	This group represents the lowest rights. The accounts in this group are authorized to issue query commands and modify their own attributes.

Group	Rights
Operator personnel	The accounts in this group are authorized to query the system information and perform some configuration operations.
Maintenance personnel	The accounts in this group are authorized to perform all maintenance operations.
Administrator	The accounts in this group are authorized to perform all query and configuration operations and security management.
Super administrator	The accounts in this group are authorized to perform all operations during expert maintenance processing, including security management.

1.4.2.3 Auditing

Logs record routine maintenance events of the TOE. Administrators can find security loopholes and risks by checking logs. Considering security, the TOE provides security logs and operation logs.

Security logs record operation events related to account management, such as modification of passwords and addition of accounts.

Operation logs record events related to system configurations, such as modification of equipment IP addresses and addition of services.

The TOE provides a Syslog solution to resolve the problem of limited equipment storage space. Currently, only security logs are saved on the Syslog server.

1.4.2.4 Communication Security

The TOE provides communication security by implementing the SSL protocol. Versions SSL3.0 and TLS1.0 are implemented. SSL certificates are required for establishing SSL and TLS encryption channels. The SSL certificates are managed and issued by carriers. The TOE loads and activates SSL certificates.

The TOE provides an SFTP client for software upgrades. In this application, the TOE serves as a client and the SFTP server is deployed outside the equipment network and is provided by the carrier.

The SFTP authentication policy is determined by the SFTP server. The TOE supports password authentication and key authentication. Password authentication is the process wherein an SFTP client uses a user name and password to log in to the SFTP server. Key authentication is the process wherein an SFTP client and SFTP server adopt Revist-Shamir-Adleman Algorithm (RSA) for cryptographic authentication. A user needs to generate an RSA key on the equipment and upload the public key to the SFTP server before cryptographic authentication. The user can set the length of the RSA key from 2048 bits to 4096 bits.

The TOE uses passphrases to protect private keys on an SFTP client for cryptographic authentication. When users generate a key pairs, they need to indicate the passphrases.

1.4.2.5 Access Control

The TOE provides Access Control List (ACL) for filtering incoming information flows to management interfaces. An administrator can set deny IP addresses and communication ports, to limit data from specific IP addresses and to filter data from specific communication ports. The ACL function protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and communication ports. The administrator can create, delete, and modify ACL rules.

Table 1-5 Classification of ACL

Item	Feature
Basic ACL	Rules are defined based on the source IP address.
Advanced ACL	Rules are defined based on the source IP address and port, destination IP address and port, IP protocol type, and ICMP type.

Table 1-6 ACL parameters

Parameter	Value Range	Description
ACL rule	0–0xffffffff	Indicates the rule number. A rule number is automatically assigned by the ACL protocol when the value is **0xffffffff**.
ACL operation type	Permit and deny	Indicates the ACL operation type. The values are as follows: • Deny: If a received message complies with a rule in an ACL, the message is discarded. • Permit: If a received message complies with a rule in an ACL, the message is forwarded.
Source IP address	Source IP address	The source IP address and the source wildcard determine the addresses to which that an ACL rule is applicable.
Source wildcard	0–0xFFFFFFFF	The value **0** represents a bit that must be exactly matched and the value **1** represents a bit that is ignored.
Destination IP address	Destination IP address	The destination IP address and the destination wildcard determine the addresses to which that an ACL rule is applicable.
Destination wildcard	0–0xFFFFFFFF	The value **0** represents a bit that must be exactly matched and the value **1** represents a bit that is ignored.

Parameter	Value Range	Description
Protocol type	TCP, UDP, ICMP, and IP	Set this parameter to **UDP** or **TCP** when you want to filter packets at an UDP or a TCP port. Set this parameter to **ICMP** when you want to filter packets of the ICMP protocol and code type. The value **IP** indicates that the protocol type is not concerned.
Source port	0–65535 or 0xFFFFFFFF; **0xFFFFFFFF** indicates that this parameter is not concerned.	This parameter is available only when **Protocol type** is set to **TCP** or **UDP**.
Destination port	0–65535 or 0xFFFFFFFF; 0xFFFFFFFF indicates that this parameter is not concerned.	This parameter is available only when **Protocol type** is set to **TCP** or **UDP**.
ICMP protocol type	ICMP protocol type	This parameter is available only when **Protocol type** is set to **ICMP**. The value **255** indicates that this parameter is not concerned.
ICMP code type	ICMP code type	This parameter is available only when **Protocol type** is set to **ICMP**. The value **255** indicates that this parameter is not concerned.

2 CC Conformance Claims

2.1 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R4.

The TOE claims EAL3+ augmented with ALC_CMC.4 and ALC_FLR.2.

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Threats

The assumed security threats are listed below.

The **information assets** to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, and audit records), and other information that the TOE facilitates access to (such as system software, patches) are all considered as part of information assets.

T.UnwantedNetworkTraffic The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exist on management plane. The Unwanted network traffic may come from an attacker and should be filtered. The overloaded traffic may cause a failure of the TOE to respond to system control and normal management operations.

T.UnauthenticatedAccess An unauthenticated person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE, exhausting system resources.

T.UnauthorizedAccess A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device.

T.Eavesdrop An eavesdropper (remote attacker) is able to intercept, and potentially modify, or re-use information assets that are exchanged between the TOE and EMS.

3.2 Assumptions

3.2.1 Physical Assumptions

A.PhysicalProtection It is assumed that the TOE (including any board attached, access of CF card) is protected against unauthorized physical access.

3.2.2 Network Elements

A.NetworkElements It is assumed that the EMS，Syslog sever and Radius Server are trusted and will not be used to attack the TOE.

3.2.3 Network Segregation

A.NetworkSegregation It is assumed that the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the application (or, public) networks where the interfaces in the TOE are accessible. And it is assumed that the transport network is trusted. It is also assumed that the EMS, Syslog server, and Radius server are trusted and will not be used to attack the TOE.

3.2.4 Personnel Assumptions

A.NOEVIL The authorized users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O. DeviceAvail** The TOE shall ensure its own availability.
- **O. DataFilter** The TOE shall ensure that only allowed management traffic goes through the TOE.
- **O.Authorization** The TOE shall implement different authorization role that can be assigned to users in order to restrict the functionality that is available to individual administrators.
- **O.Authentication** The TOE must authenticate users for access.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.Communication** The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.

4.2 Security Objectives for the Operational Environment

- **OE.Physical** The TOE (i.e., the complete system including attached peripherals, such as a board, and CF card inserted in the transmission equipment) shall be protected against unauthorized physical access.
- **OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, EMS used for TOE management, Syslog servers, and Radius servers for obtaining authentication and authorization decisions.
- **OE.NetworkSegregation** The operational environment shall provide segregation by deploying the management interface in TOE into an independent local network.
- **OE.Person** Personnel working as authorized administrators shall be carefully selected for trustworthyness and trained for proper operation of the TOE.

4.3 Rationale for Security Objectives

The following table provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat.

Table 4-1 Mapping objectives to threats

Threat	Security Objectives	Rationale for Security Objectives
T.UnwantedNetworkTraffic	O.DeviceAvail O.DataFilter	This threat is countered by O.DeviceAvail, ensuring that the TOE remains available, and O.DataFilter ensuring that unwanted data is filtered and cannot access the network resources.
T.UnauthenticatedAccess	O.Authentication O.Audit	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).
T.Unauthorized Access	O.Authorization O.Audit	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).
T.Eavesdrop	O.Communication	The threat of eavesdropping is countered by requiring communications security via SSL and SFTP for communication between EMS and the TOE (O.Communication).

The following table provides a mapping of the objectives for the operational environment to assumptions and threats, showing that each objective is at least covered by one assumption or threat.

Table 4-2 Mapping objectives for the environment to threats and assumptions

Environmental Objective	Threat /Assumption
OE.Physical	A.PhysicalProtection

Environmental Objective	Threat /Assumption
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation
OE.Person	A.NoEvil

4.4 Extended Components Definition

No extended components have been defined for this ST.

5 Security Requirements for the TOE

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.

5.2 Security Functional Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 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:

1. All auditable events for the [***not specified***]level of audit; and
2. **[The following auditable events recorded to operation logs:**
   - **i. user activity**
     - **login, logout**
     - **configuration operation set requests**

   The following auditable events recorded to security logs:
   - **ii. user management**
     - **add, delete, modify users**
     - **user password change**
     - **user operation authority change]**

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

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**Operation Type (if applicable)**, **Operation Object(if applicable), Access IP Address(if applicable)**, **User Name (if applicable)].**

5.2.1.2 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 causes the event.

5.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **[users authorized Administrator group]** with the capability to read **[all information]** from the audit records.

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

5.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.5 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.

5.2.1.6 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall **[roll back the oldest records]** if the audit trail exceeds **[the size of the storage device].**

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **[user group role]** on

[Subject: users;

Objects: commands /features provided by TOE;

Operation: Read access / write access /Deny access]

5.2.2.2 FDP_ACF.1 Security Attribute based Access Control

FDP_ACF.1.1 The TSF shall enforce the **[user group role]** to objects based on the following:

[Subject security attributes

users and their following security attributes:

- **user Identity**
- **user level assignment**

Objects security attributes:

commands and their following security attributes:

- **Commands and command level]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

1. **Only authorized users are permitted access to commands and feature.**
2. **Users can be configured with different user group role to control the device access permission.**
3. **There are five user group roles including Monitor, Operator, Maintainer, Administrator, Super administrator, in ascending order of priorities.**
4. **User group role map command levels. A user can only run commands at the same or lower level.**
5. **A command level is defined by the software.]**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[**

the user has been granted authorization for the relevant level commands]

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

1. **the user has not been granted authorization for the commands targeted by the request, or**
2. **the user is not granted authorization with a Command beyond user relevant level].**

5.2.2.3 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **[the authentication information of SSL,SFTP]**

FDP_DAU.1.2 The TSF shall provide **[SSL,SFTP]** with the ability to verify evidence of the validity of the indicated information.

5.2.2.4 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1(1) The TSF shall enforce **[ACLs]** on

[Subjects:

TOE management interface through which traffic goes

Information:

Traffic flows;

Operations:

Permit, Deny]

5.2.2.5 FDP_IFF.1 Simple Security Attributes

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

Subject: TOE interface through which management traffic goes

Information security attributes:

Packet characteristic: such as Source IP address / Destination IP address / protocol type /Source port / Destination port.etc.]

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: [**Network traffic is match TOE according to administratively configured policies**

The specific information flow control rules associated with each policy are as follows:

ACL

Ingress or egress IP traffic with security attributes that match configured ACL policy rule will be processed according to that rule.]

FDP_IFF.1.3 The TSF shall enforce the **[none].**

FDP_IFF.1.4 The TSF shall explicitly authorize 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:**[**

For ACL feature, packets that match configured ACL with action "deny" are dropped]

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **[*five*]** unsuccessful authentication attempts occur (and the interval between two attempts is shorter than three minutes) related to **[user logging in]**.

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

1. **the User Identification which is existed in the TOE is locked**
2. **report the ALARM].**

5.2.3.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

1. **user ID**
2. **user level**
3. **password]**

5.2.3.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1/a The TSF shall provide a mechanism to verify that secrets meet **[for Certificates used as seeds for building encrypted SSL/TLS channels]**

FIA_SOS.1.1/b The TSF shall provide a mechanism to verify that secrets meet **[for password for user authentication for authentication and they are case sensitive. A cipher password mode should be used and the length of password should be at least 8 characters long, and the password should be at least contains three of capital letter, small letter, number, and special character.]**

5.2.3.4 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [**establishment of a secure remote session between the administrative user and the TOE component]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.5 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide **[the following authentication mechanisms:**

1. **Remote authentication by RADIUS;**
2. **Local Authentication by local database of TOE]**

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's identity according to the following: [

1. **For Remote authentication by RADIUS**
2. **For local Authentication, the TSF will authenticate the administrator based on the configured Identification and Authentication group].**

5.2.3.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[establishment of a secure remote session between the administrative user and the TOE component]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behavior of*]** all the functions **[defined in FMT_SMF.1]** to **[the group-defined roles]**.

5.2.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the **[user group role]** to restrict the ability to ***[query, modify]*** the security attributes **[identified in FDP_ACF.1 and FIA_ATD.1]** to the **[group-defined roles]**.

5.2.4.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the **[user group role]** to provide ***[restrictive]*** default values for security attributes (Command Group associations) that are used to enforce the SFP.

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

5.2.4.4 FMT_SMF.1 Specification of Management Functions

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

1. **authentication, authorization**
2. **ACL policy**
3. **user management**
4. **query audit records]**

5.2.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **[group-defined roles]** (refer to table1- 4)**.**

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

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_STM.1 Reliable Timestamps

FPT_STM.1.1 The TSF shall be able to provide reliable timestamps.

5.2.6 TOE access (FTA)

5.2.6.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **[a time interval of user inactivity which can be configured.]**

5.2.6.2 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[**

1. **authentication failure**
2. **Source IP address doesn't match IP address configured in ACL for user management.]**

5.2.7 Trusted Path/Channels

5.2.7.1 FTP_ITC.1 Trusted Channel(SFTP)

FTP_ITC.1.1 The TSF shall provide a communication path between itself and (SFTP) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the TSF]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted path for **[download software for upgrade]**

5.2.7.2 FTP_ITC.1 Trusted Channel (SSL)

FTP_ITC.1.1 The TSF shall provide a communication path between itself and (EMS) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the EMS]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted path for **[EMS management]**.

5.2.7.3 FTP_ITC.1 Trusted Channel (WebLCT)

FTP_ITC.1.1 The TSF shall provide a communication path between itself and (WebLCT) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the WebLCT]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted path for **[WebLCT management]**.

5.2.7.4 FTP_ITC.1 Trusted Channel (Mobile LCT) (for RTN products only)

FTP_ITC.1.1 The TSF shall provide a communication path between itself and (mobile LCT) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[the mobile LCT]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted path for **[mobile LCT management]**.

5.3 Security Functional Requirements Rationale

5.3.1 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 5-1 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_DAU.1	No Dependencies	None
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No Dependencies	None
FIA_SOS.1	No Dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	No Dependencies	None
FIA_UID.1	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTP_STM.1	No Dependencies	None

Security Functional Requirement	Dependency	Resolution
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_ITC.1(SFTP)	No Dependencies	None
FTP_ITC.1(SSL)	No Dependencies	None
FTP_ITC.1(WebLCT)	No Dependencies	None
FTP_ITC.1(Mobile LCT)	No Dependencies	None

5.3.2 Sufficiency and Coverage

Table 5-2 Mapping of objectives to SFRs

Objective	SFR	Rationale
O.DeviceAvail O.DataFilter	FDP_IFC.1 FDP_IFF.1	These SFRs also apply ACL to limit packets going to Management Plane through the TOE, further ensuring availability of TOE and network resources.
O.Communication	FTP_ITC.1(SFTP)	This SFR provides secure communication channels between SFTP and the management interface of the TOE.
	FTP_ITC.1(SSL)	This SFR provides secure communication channels between the TOE and EMS.
	FTP_ITC.1(WebLCT)	This SFR provides secure communication channels between the TOE and WebLCT.
	FTP_ITC.1(Mobile LCT)	This SFR provides secure communication channels between the TOE (RTN products) and the Mobile LCT.
	FDP_DAU.1 FIA_SOS.1	These SFRs provide secure communication channels between the TOE and EMS/SFTP.
O.Authentication	FIA_UID.1 FIA_UAU.1 FIA_UAU.5	These SFRs ensure that a user must identify and authenticate himself, either by a local password or through the RADIUS server.
	FTA_TSE.1 FIA_AFL.1 FTA_SSL.3	These SFRs support authentication by: • Refusing logins from certain IP addresses. • Not allowing unlimited login attempts. • Logging out users after an inactivity period. • Ensuring password quality.

Objective	SFR	Rationale
O.Authorisation	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized admins can access certain functions.
	FMT_SMR.1 FIA_ATD.1	These SFRs defines authorization role and ensure that upon login an administrator gets the proper authorization level.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization level.
	FMT_MSA.1 FMT_MSA.3	These SFRs ensure that new admins only get limited access rights and specify who can modify these access rights.
O.Audit	FAU_GEN.1, FAU_GEN.2 FPT_STM.1	These SFRs ensure that audit records can be generated for significant events and that these records contain useful information, including the correct time of the events.
	FAU_SAR.1, FAU_SAR.2	These SFRs ensure that correct users can read correct information from audit records.
	FAU_STG.1, FAU_STG.3	These SFRs ensure audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.

5.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3+ components augmented with ALC_CMC.4 and ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

5.5 Security Assurance Requirements Rationale

The evaluation assurance level 3+ augmented with ALC_CMC.4+ALC_FLR.2, has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

6 TOE Specification Summary

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

6.1.1 Authentication

The TOE can identify users based on unique IDs and enforce their authentication before granting them access to any TSF management interfaces. Detailed functions include:

- Support authentication via local passwords. This function is achieved by comparing user information input with pre-defined user information stored in the flash.
- Support authentication via the remote RADIUS authentication server. This function is achieved by performing pass/fail action based on the result from the remote authentication server.
- Support authenticated user logins using the SSL mode.
- Support logout when no operation is performed on the user session within a specified interval. If an account that has logged in does not exchange information with the EMS and TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login.
- Support maximum attempts for authentication failures within certain period of time. After five login attempts using one account fail and the interval between two attempts is shorter than 3 minutes, the account is locked. An alarm is reported after the account is locked.
- Support access limit by IP address. A series of whitelists and blacklists are set to filter IP addresses and data on communication ports. Unauthorized IP addresses and communication ports cannot access the system.
- Support for user individual attributes including the user ID, user level, and password to ensure that each user is unique in the system.

(FDP_DAU.1, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1, FTA_SSL.3, FTA_TSE.1, FTP_TRP.1)

6.1.2 Authorization

The TOE enforces an access control by supporting following functions:

- Support five access role groups.
- Support assigning an access group to accounts.

- Accounts are managed in groups. The accounts in the super administrator group are authorized to perform all security management and maintenance operations. They have the highest authority and can only be used in fault diagnosis scenarios. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is logged.

(FDP_ACC.1, FIA_ATD.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1)

6.1.3 Auditing

The TOE can provide auditing by means of operation logs and security logs:

- Support recording non-query operations in the operation logs, including the operation type, operation object, and access IP address user name.
- Support recording security-related configuration operations in the security logs, including user management, security settings, and the attempts of unauthorized operations. The security logs provide the information about the account name, address of the client, time, and operation.
- Only authorized accounts higher than the administrator level can query and dump operation logs.
- The system checks the integrity of the operation logs and allows no manual changes.
- The operation logs can be completely recovered even after a power-outage restart of the system.
- The operation logs keep records in time sequence. After the memory is exhausted, the earliest records of the operation log are overwritten by the latest records. Once the memory is exhausted, a performance event is reported.

(FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3)

6.1.4 Communication Security

The TOE provides communication security by implementing SSL. The SSL3.0/TLS1.0 protocol is implemented to provide communication channels. The SSL certificates are managed and issued by carriers. The TOE supports SSL certificate loading and activation. The TOE has been loaded with a preset SSL certificate before delivery. SFTP provides the secure file transfer functionality.

- Support SSL tunnel from EMS to the transmission Equipment. This tunnel can be direct or indirect (via other TOEs).
- Support SSL tunnel from the Mobile LCT to the RTN products.
- Support Secure-FTP.

(FMT_SMF.1, FDP_DAU.1, FIA_SOS.1, FTP_ITC.1(SFTP), FTP_ITC.1(SSL), FTP_ITC.1(WebLCT), FTP_ITC.1(Mobile LCT))

6.1.5 Access Control

The TOE uses ACL to deny unwanted network traffic on management interfaces.

IP-based ACL is provided to filter traffic flow on management interface by matching all or some attributes, including the source IP address, destination IP address, IP protocol number,

TCP/UDP source port number, and TCP/UDP destination port number, and then performs actions such as rate limit, prioritization, or discard accordingly.

(FDP_IFC.1, FDP_IFF.1)

6.1.6 Security Management

The TOE allows management of the telecommunications network by different users. The TOE can be configured to grant each user the access right to the telecommunications network resources that are required for user operations. The functions include:

- User management, including the user name and passwords.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of SSL for the communication between EMS and the TOE.
- Definition of IP addresses and address ranges for clients that are allowed to connect to the TOE.

All of these management options are generally available via the EMS.

Detailed functions include:

- Support remote TOE management using SSL.
- Support S-FTP enable and disable.
- Support automatic account logout when no operation is performed on the user session within a specified interval.
- Support the maximum attempts for authentication failures within certain period of time.
- Support access limit by IP address.
- Support ACL filtering based on IP protocol number, source and/or destination IP address, or source and/or destination port number.
- Support configuration of the RADIUS server.
- Support configuration of the Syslog server.

(FMT_SMF.1)

6.1.7 Time

The TOE provides its own clock and timestamps to correctly record logs in time sequence.

(FPT_STM.1, FTA_SSL.3)

A Abbreviations, Terminology and References

A.1 Abbreviations

CC	Common Criteria
LMT	Local Maintenance Terminal
EMS	Element Management System
NMS	Network Management System
USP	Universal Software Platform
LCT	Local Craft Terminal
PP	Protection Profile
RMT	Remote Maintenance Terminal
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
RSA	Rivest Shamir Adleman
RADIUS	Remote Authentication Dial-In User Service
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
MSTP	Multi-Service Transmission Platform
SDH	Synchronous Digital Hierarchy
WDM	Wavelength Division Multiplexing

OTN	Optical Transport Network
RTN	Radio Transmission Node
OSN	Optical Switch Node

A.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

Operator See User.

User: A user is a human or a product/application using the TOE.

A.3 References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, . Version 3.1 Revision 4, September 2012

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 4, September 2012