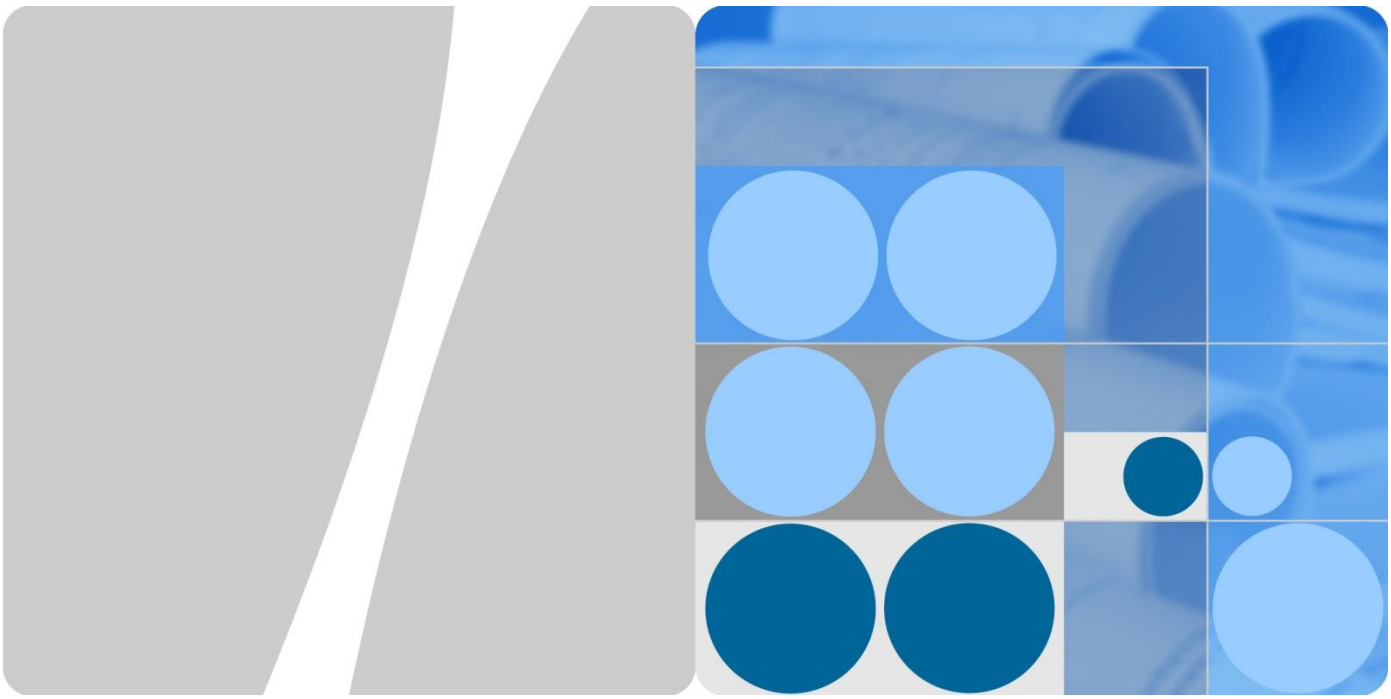


CC Security Target Lite

for Huawei OptiX OSN 1800 V V100R006C20 software management component

Issue	1.53
Date	2018-10-10

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

About This Document

Purpose

This Security Target is for the evaluation of OptiX OSN 1800 V V100R006C20 software management component, consisting of unified transmission software (UTS), and underlying OS. The software is part of OptiX OSN 1800 V.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Contents

Figures

Tables

1 Introduction

This Security Target is for the evaluation of OptiX OSN 1800 V V100R006C20 software management component, consisting of unified transmission software (UTS), and underlying OS(Operation System). The software is part of OptiX OSN 1800 V.

1.1 ST Identification

Title: Security Target Lite for Huawei OptiX OSN 1800 V V100R006C20 software management component

Version: 1.53

Date: 2018-10-10

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei OptiX OSN 1800 V V100R006C20 software management component

Version: V100R006C20

Developer: Huawei Technologies Co., Ltd.

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 is part of the OptiX OSN 1800 V software which is the software running on the OptiX OSN 1800 V device. The TOE only consists of the unified transmission software (UTS), and underlying OS as described in the following chapters and is referred as OptiX OSN 1800 V software management component in this ST.

The OptiX OSN 1800 V device is targeted for metro edge node applications. It supports OTN, packet, and TDM services and can interconnect existing WDM equipment for the service extension purpose.

The identifier for chassis hardware used for testing of the software TOE is OptiX OSN 1800V chassis (see Table 1-1).

Table 1-1 lists the available chassis of OptiX OSN 1800 V.

Table 1-1 Chassis of OptiX OSN 1800 series

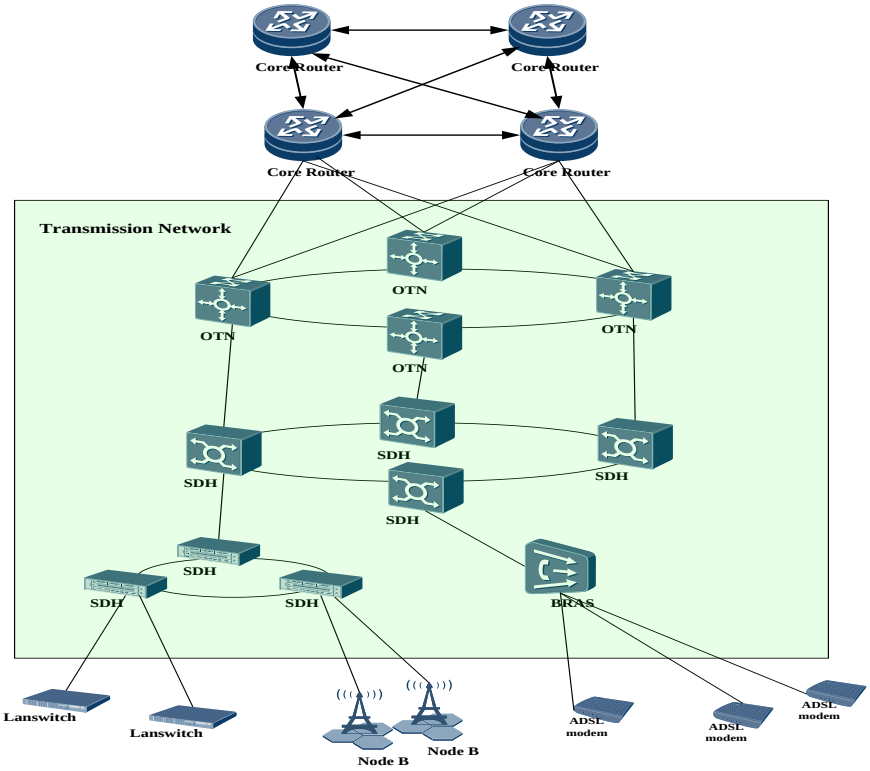
Chassis	Product Version
OptiX OSN 1800 V	V100R006C20

The identifier for the System Control and Communication unit hardware revision used for testing of the software TOE is TNZ5UXCMS.

1.3 Product overview

Transmission networks (including SDH, 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 transmission network on the entire communication network



Located at the transmission 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, since the TOE is only the management component and, therefore, its TSF provide no measure of protecting transmission traffic.

A Metropolitan Area Network is generally a communication network built within a city, which is divided into three layers:

- the access layer of the metropolitan area network,
- the aggregation layer of the metropolitan area network, and
- the core layer of the metropolitan area network.

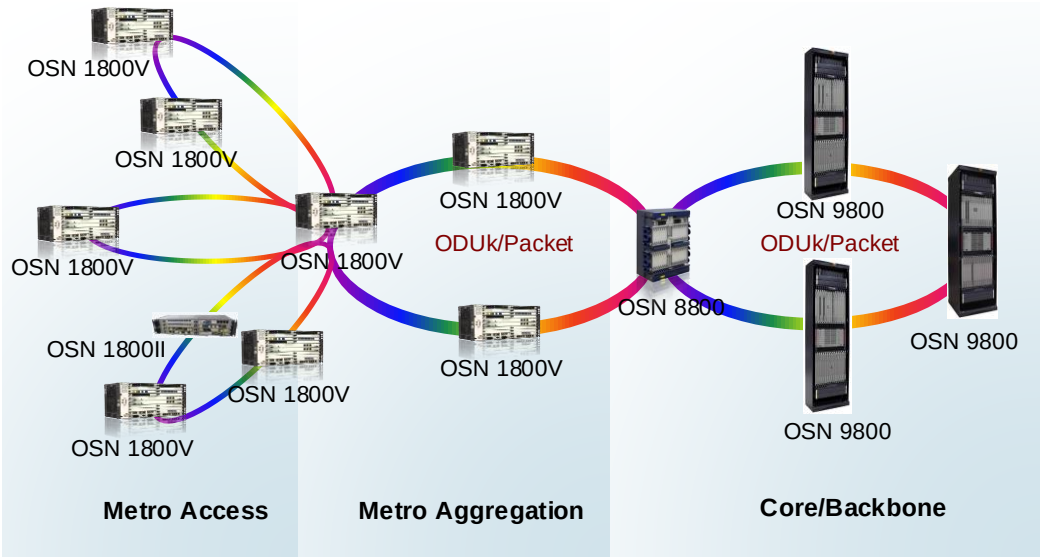
The access layer of the metropolitan area network is mainly responsible for the access control of the services of individual and enterprise users. The aggregation layer of the metropolitan area network is to converge the massive user traffic and connect the access layer and core layer of metropolitan area network. The role of the core layer of the metropolitan area network is to provide the export of the metropolitan area network, connect with all backbone networks, and connect with the Internet Data Center of the city. Backbone networks are high-speed networks used to connect multiple regions' networks such as metropolitan area networks or other backbone networks.

The OptiX OSN 1800V device is mainly applicable to the access layer of the metropolitan area network and the aggregation layer of the metropolitan area network, which is responsible for accessing and converging the services of individual and enterprise users into metropolitan area networks. Services such as OTN, Packet, and SDH services are processed at the access layer and then sent to the convergence node on the metro transmission network. In this manner, the OptiX OSN 1800 V works with the current OptiX WDM equipment to extend the services to the access layer. On a network with a small capacity, the OptiX OSN 1800 V is also applicable to the backbone layer.

The OptiX OSN 1800 V uses dense wavelength division multiplexing (DWDM) and coarse wavelength division multiplexing (CWDM) technologies to groom wavelengths at each node. The OptiX OSN 1800 V features easy capacity expansion, flexible service access, high bandwidth utilization, and high reliability.

The OptiX OSN 1800 V can form an MS-OTN network with the OptiX OSN 8800, OptiX OSN 9800, or OptiX OSN 1800 II. Figure 1-2 shows the position of the OptiX OSN 1800 V on the entire network.

Figure 1-2 Position of the OptiX OSN 1800 V on the entire network



1.4 TOE Type and TOE Overview

The OptiX OSN 1800 V device is transmission equipment and is mainly applicable to the access layer of the metropolitan area network and the aggregation layer of the metropolitan area network . It is generally deployed in the upstream of wired broadband and mobile carrier facilities, which consists of software and hardware.

The hardware is composed of cabinet, chassis, power unit, and boards. The cabinet is used to install chassis and power units. The power unit is used to supply power to the chassis. The chassis provides the board slot to insert boards.

Boards are the core unit of processing and management in transmission equipment, consisting of SCC (System Control and Communication) unit and service unit, consisting of OTN line board, Optical layer board, Packet board, and TDM board etc.

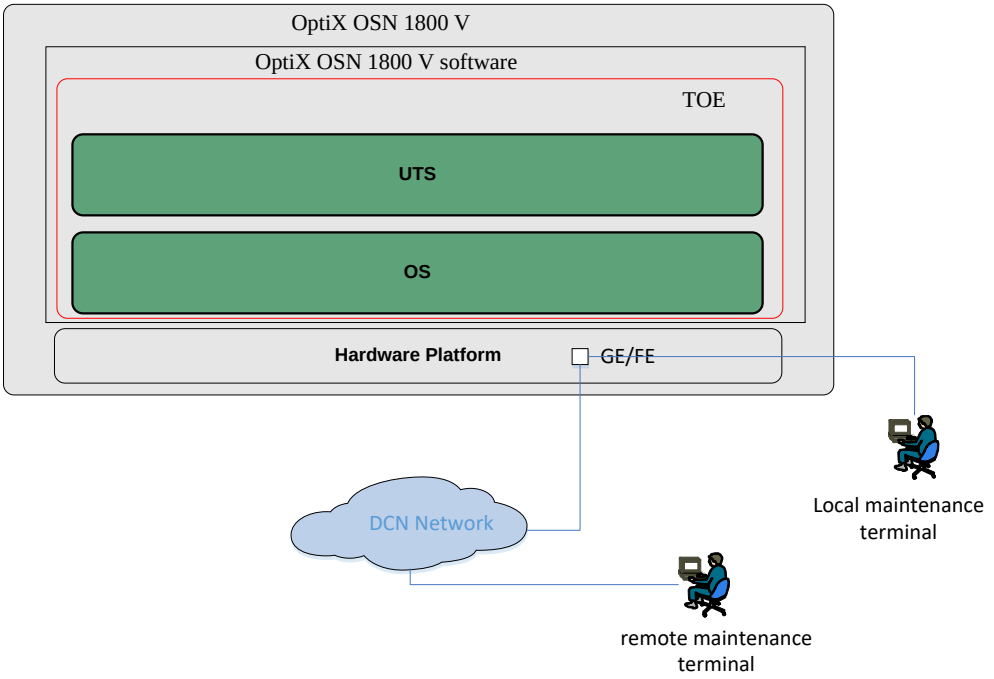
The SCC (System Control and Communication) unit is the center of the system. It collaborates with the EMS (Element Management System) to centralize control and manage all service units of the system and implement inter-equipment communication. All service units are centrally managed and controlled by the SCC unit, in which independent control and management software is running. The EMS manages OptiX equipment using a GUI interface. The GUI interface complies with a special management protocol defined by Huawei exclusively for OptiX equipment.

The OptiX OSN 1800 V software is deployed in the SCC unit and service units, which is responsible for the system management and control and service transmission.

The TOE type is a transmission software platform, which is part of the OptiX OSN 1800 V software. It consists of the Unified Transmission Software (UTS) component, which is the platform software, and the underlying OS for the System Control and Communication unit (TNZ5UXCMS) as shown in figure 1-3. These components provide the core control and management services of the device.

The non-TOE SW components include system and service attribute management, service schedule and protect, optical Layer protocol, service warning and performance, and service control and monitor.

Figure 1-3 TOE constitution



The UTS is responsible for managing and controlling the whole OptiX OSN 1800 V software, communication, and security features in OptiX OSN 1800 V. The UTS is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc. Because the UTS mainly provides the security feature of the TOE, the aspects evaluated are the unified transmission software (UTS), and underlying OS of the OptiX OSN 1800 V.

To counter the security threats of OptiX OSN 1800 V, the unified transmission software (UTS) deployed in SCC unit provides many security measures to mitigate security risks effectively. The main security features are:

1. Identification and authentication of administrative users
2. Authorization
3. Auditing
4. Communication Security
5. Access Control
6. Cryptographic functions
7. Security functionality management

The detailed description of above security features is in the chap.1.5.

1.5 TOE Description

This chapter provides an architectural overview of OptiX OSN 1800 V device including a detailed description of the physical architecture and the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

1.5.1 Architectural overview of OptiX OSN 1800 V

This section will introduce OptiX OSN 1800 V from a physical architectural point of view and a software architectural point of view.

1.5.1.1 Physical Architecture of OptiX OSN 1800 V

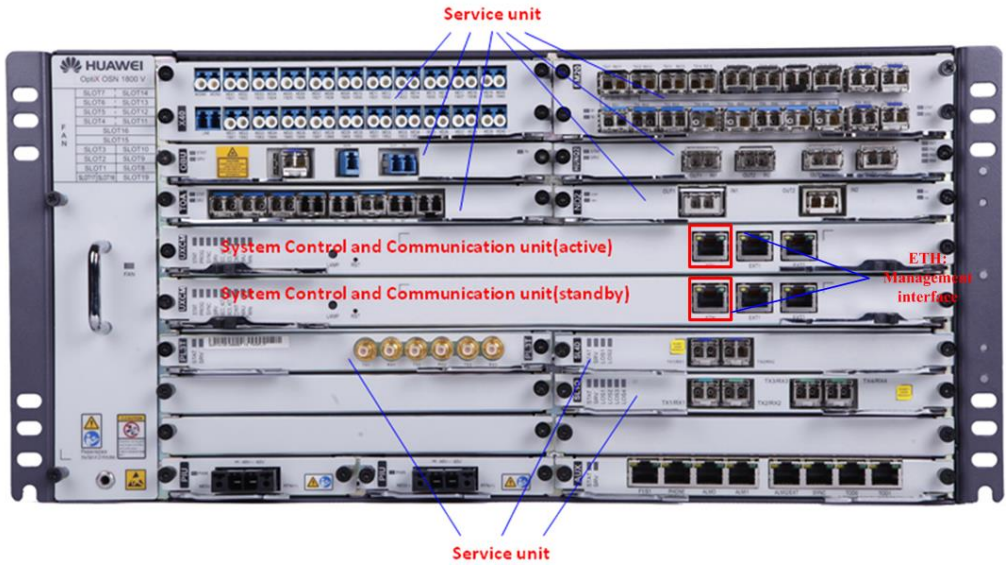
The OptiX OSN 1800 V is transmission equipment and is mainly applicable to the access layer of the metropolitan area network and the aggregation layer of the metropolitan area network. Services such as OTN, Packet, and SDH services are processed at the metro access layer and then sent to the convergence node on the metro transmission network.

The OptiX OSN 1800 V device consists of the hardware and the software.

The hardware is composed of cabinet, chassis, power unit, and boards. The cabinet is used to install chassis and power units. The power unit is used to supply power to the chassis. The chassis provides the board slot to insert boards.

Boards are the core unit of processing and management in transmission equipment, consisting of SCC (System Control and Communication) unit and service unit, consisting of OTN line board, Optical layer board, Packet board, and TDM board etc.

Figure 1-4 System architecture of the OptiX OSN 1800 V



The service units are responsible for signal amplifying, optical transpondering, optical multiplexing and demultiplexing, optical add and drop multiplexing etc., in which a board software is running.

The SCC (System Control and Communication) unit is the center of the system. It collaborates with the EMS to centralize control and manage all service units of the system and implement inter-equipment communication. All service units are centrally managed and

controlled by the SCC unit, in which independent control and management software is running.

The OptiX OSN 1800 V software is deployed in the SCC unit and service units. The part of the OptiX OSN 1800 V software deployed in the SCC unit includes UTS and other service application components. UTS is a platform software, which is responsible for managing and controlling the all software units, and is responsible for communication with external management network entities including EMS (Element Management System), RADIUS server, SFTP server and syslog server etc., and provide all security features to ensure the security of the OptiX OSN 1800 V device.

The UTS is relying on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc.

1.5.1.2 Software Architecture of OptiX OSN 1800 V

In terms of the software, OptiX OSN 1800 V's software architecture consists of two logical planes to support centralized controlling and management and transparent transmission mechanism:

- Data plane
- Control and management plane

The **control and management plane** is the core of the entire system. It controls and manages the system. The control and management unit processes protocols and signals, configures and maintains the system status, and reports and controls the system status.

The **data plane** is responsible for high speed processing and non-blocking forwarding of data packets. It encapsulates or decapsulates packets, transparently transmits them, and collects statistics.

The unified transmission software (UTS) and the underlying OS are the control and management core that runs on the SCC unit, which is responsible for managing and controlling the whole OptiX OSN 1800 V software, communication, and security features in OptiX OSN 1800 V.

OptiX OSN 1800 V handles L0, L1, and L2 traffic transmissions, which are handled by the service units without additional security related control or management functionality.

1.5.2 Scope of Evaluation

This section will define the scope of the part of OptiX OSN 1800 V comprising the TOE to be evaluated.

1.5.2.1 Physical scope

The TOE is a 'software only', TOE consists of the unified transmission software (UTS) and underlying OS of the OptiX OSN 1800 V, but not the hardware, which the UTS and underlying OS is running on. This will be discussed in more detail in the next chapter. In addition, the software package, signature file, and the guidance documentation are delivered in CD-ROM:

Type	Delivery Item	Version
Software	OptiX OSN 1800 V100R006C20SPC300 Software.zip SHA-256 checksum: 2acd6990d24786dc7b27b35e6111b3e97e7203b53a2a648af7fdf302bdb6f8bc	V100R006C20SPC300
Software Signature File	OptiX OSN 1800 V100R006C20SPC300 Software.zip.asc	-
Product Guidance	OSN 1800 V & 1800 I II Compact V100R006C20 Deploying Your Network	Issue 03
	CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_OPE	V0.5
	CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_PRE_Production	V0.4
	CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_PRE_User	V1.1
	Huawei OptiX OSN 1800 V V100R006C20 Software Configuration and Reference	V0.7

1.5.2.2 Logical scope

The TOE boundary from a logical point of view is represented by the elements that are displayed with a red frame within the rectangle in the figure below. The TOE only consists of unified transmission software (UTS), and the underlying OS, see red frame in Figure 1-5. As shown in Figure 1-4, the SCC unit hosts the TOE. The TOE is running on the eight cores of the CPU. The service unit (including OTN line board, Optical layer board, Packet board, and TDM board etc) does not contain parts of the TOE. The TOE provides several security functions, which are described in more detail in chap.1.5.3 .

Figure 1-5 TOE logical scope

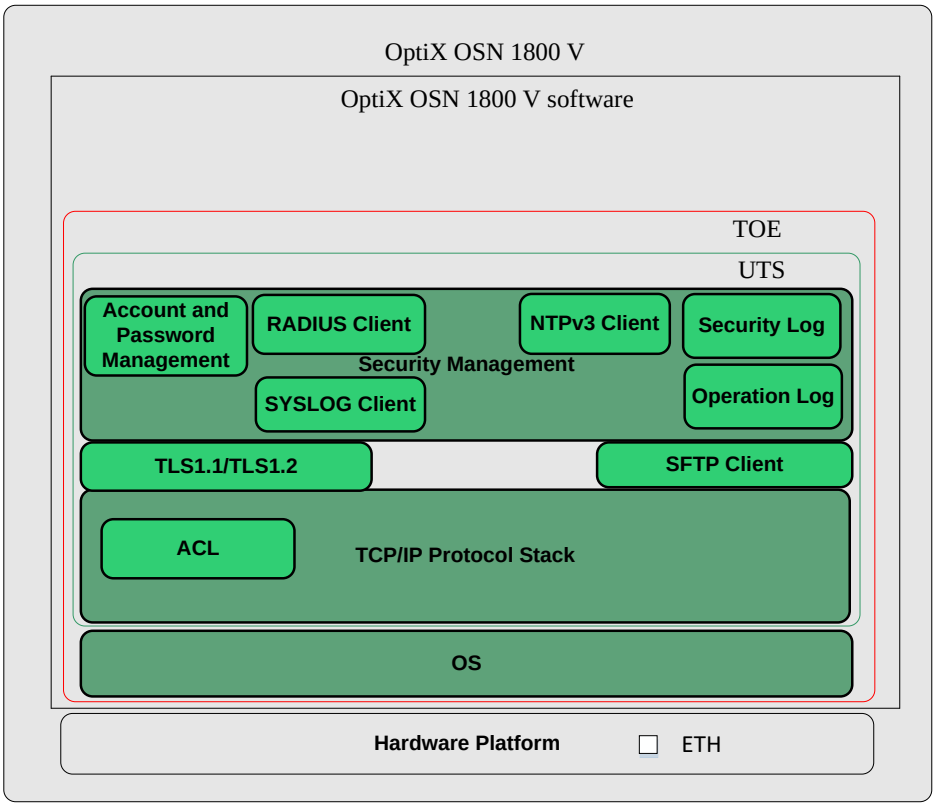


Figure 1-5 reflects also the basic structure of the TOE with respect to subsystems.

The TOE provides all the security functions.

The TOE also controls the flow of management network traffic between network interfaces by matching information contained in the headers of network packets against routing table in forwarding engine.

System control and security management are performed either through LMT which is connected to the Management plane of the TOE directly via the GE/FE Ethernet port or through RMT via a secure channel enforcing TLS1.1/1.2 via the GE/FE port on the SCC unit through the DCN network.

1.5.2.3 Non-TOE Hardware and Software

Based on physical scope and logical scope described so far, a list of configuration is to be added:

- For management via the ETH interface, authentication is always enabled. Authentication mode is Authentication, Authorization, Accounting (‘AAA’, i.e. username and password). Length of password is no less than 8 characters.
- Service of FTP have to be disabled to use the TOE in the certified configuration.

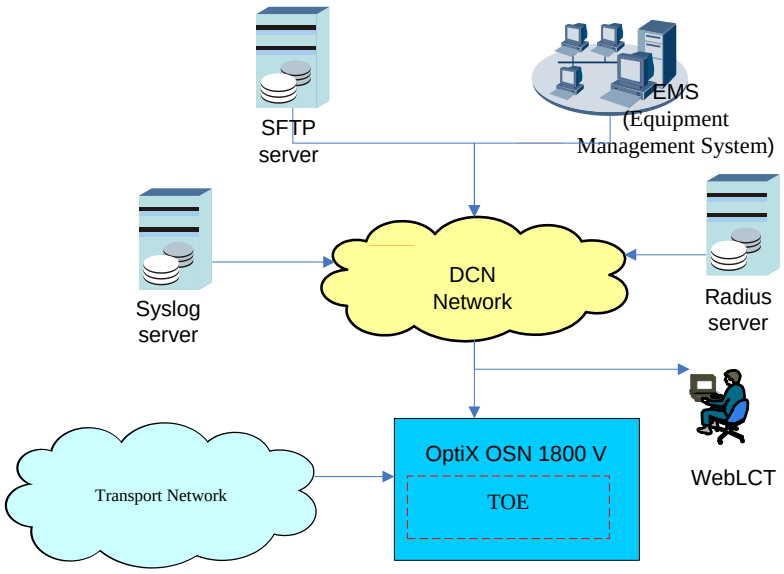
The environment for TOE comprises the following components:

- Local PCs (WebLCT) used by administrators to connect to the TOE for access through interfaces on SCC unit via a secure channel of TLS, or non-secure channel. Access will be performed using a command line terminal.
- Remote PCs used by administrators to connect to the TOE for access through interfaces on

SCC unit within the TOE via a secure channel of TLS.

- Since the TOE is part of the OptiX OSN 1800 V device, and it can only operate as part of the device, which means that all non-TOE parts of the device are also required. Furthermore, the TOE requires an EMS (Element Management System, it typically runs the U2000 rich user interface management software), a syslog server and an SFTP Server, as shown in the following figure. A Radius server is optional and may be used instead of local authentication.

Figure 1-6 The TOE in its operational environment



1.5.3 Summary of Security Features

1.5.3.1 Identification and authentication

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

The TOE provides a local authentication mode, or can optionally enforce authentication decisions obtained from a Radius server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login. In RADIUS authentication mode, accounts and passwords are saved on the RADIUS server and authenticated by the RADIUS server. During login, the accounts and passwords are forwarded to the RADIUS server, using the RADIUS protocol and the RADIUS server checks the validity of accounts and passwords.

User authentication is always enforced for EMS sessions via TLS sessions. The use of TLS connection is always required for accessing the TOE via RMT. For LMT no logically secured communication channel is required.

1.5.3.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their validity.

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

Only authenticated users can execute commands of the TOE. Only one user group level can be assigned to a user account. So the user group level of a user is unambiguous at any time. All authenticated users of the TOE are administrative users of some kind belonging to one of the user groups defined below. There are no authenticated non-administrative users.

Accounts are managed in groups and each group represents a specific authority assigned to the accounts in the group. Table 1-2 lists the groups and their definition. For example, the accounts of the "administrator" group are authorized to perform all security management and advanced diagnosis operations. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account attempts to perform any unauthorized operation, an error message is displayed and the attempt is logged.

Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging operations.

Table 1-2 Groups of accounts

Group	Authority
Monitor	This group has the lowest authority. The accounts of this group are authorized to issue query commands and modify some of their own attributes.
Operator	The accounts of this group are authorized to query the system information and perform some configuration operations.
Maintenance	The accounts of this group are authorized to perform all maintenance operations, including the authority of Operator group and general maintenance and diagnosis operations
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations. Especially, administrators can create super administrator account.
Super administrator	The accounts in this group are authorized to perform all operations of Administrator group and the advanced diagnosis (debug) operation.

Note: user level in the following content is same as user group; in CC terminology, these are considered roles.

1.5.3.3 Auditing

Logs record routine maintenance events of the TOE. Administrators can find security vulnerabilities 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. Both security logs and operation logs can be saved on an external Syslog server.

1.5.3.4 Communication Security

The TOE provides communication security by implementing the TLS protocol. TLS version 1.1 and 1.2 are implemented. TLS certificates are required for establishing TLS encryption channels. The TLS certificates are managed and issued by carriers. SFTP (description as below) is used to load TLS certificates onto TOE before establish TLS communications. The TOE acts as server during the TLS communication established between the TOE and EMS, that is to say, the EMS will validate the certificate from the TOE. The TOE does not provide path validation capabilities for X.509 certificates.

The TOE provides an SFTP client for secure file downloading and uploading. Users can use the SFTP client for fault collection, log uploading, and uploading and downloading of a file and a database etc. 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. The password authentication indicates that an SFTP client logs in to a server using an account name and a password. The key authentication indicates that an SFTP server authenticates a client using the RSA key. For the key authentication, users need to generate the RSA key on the TOE first and upload the public key to the SFTP server. The length of the RSA key ranges from 2048 to 4096 bits and is specified by users.

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

1.5.3.5 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 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 ports. The administrator can create, delete, and modify ACL rules.

Table 1-3 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 of a data packet, destination IP address of a data packet, protocol type of the IP bearer network, and protocol features. The protocol features include source port of the TCP protocol, destination port of the TCP protocol, and ICMP protocol type.

Table 1-4 ACL parameters

Parameter	Value Range	Description
ACL rule ID	0–0xFFFFFFFF	Indicates the ACL rule ID. The value 0xFFFFFFFF indicates that the ACL rule is automatically allocated by the ACL protocol or is manually assigned.
ACL operation type	Permit and deny	Indicates the ACL operation type. The values are as follows: • Deny: If a received message does not comply 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 discarded.
Source IP address	Source IP address	The source IP address and the source wildcard determine the addresses to which an access control 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.
Sink IP address	Sink IP address	The destination IP address and the sink wildcard determine the addresses to which an access control rule is applicable.
Sink wildcard	0–0xFFFFFFFF	The value 0 represents a bit that must be exactly matched and the value 1 represents a bit that is ignored.
Protocol type	TCP, UDP, ICMP, and IP	Set this parameter to UDP or TCP when filtering packets at a UDP or a TCP port. Set this parameter to ICMP when filtering 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**.
Sink 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.

Parameter	Value Range	Description
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.

1.5.3.6 Cryptographic functions

The TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (TLS, SFTP) and I&A functions (certificates, SFTP public key authentication). The TOE is capable of generating the necessary keys (AES, RSA) or importing them into the TOE. For key generation, the TOE can use its own deterministic random number generator, which is seeded from the hardware TPM of its platform.

Details of the algorithms, key lengths and modes of operation are provided in section 7.8 .

1.5.3.7 Security functionality management

Security functionality management include not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

The functions mainly include:

- Management of user accounts and user attributes, including user credentials.
- Management of authentication failure policy
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces
- Management of ACLs and ACL attributes and parameters like IP addresses or address ranges
- Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP
- Management of the TOE's time

All security management functions (i.e. commands related to security management) require sufficient user level for execution (see description of access control for details, chap. 1.5.3.2).

2 CC Conformance Claims

2.1 CC Conformance Claim

This ST is *CC Part 2 extended* [CC], extended by security functional components as defined in chap. 5, and *CC Part 3 conformant* [CC]. The version of [CC] is 3.1R5.

The ST claims conformance to the EAL2 assurance package.

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Asset

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

1. Audit data: The data which is provided by the TOE during security audit logging
2. Auth data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
3. Crypto data: The data which is used by the TOE for digital signature handling and encryption/decryption purposes.
4. Control data: The data which is used by the TOE for system software, patches update, and identity checking purposes
5. Configuration data for the TOE, which is used for configuration data of security feature and functions
6. Management Traffic data, which is the management information exchanged between the TOE and the EMS from authorized users.

3.2 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment.

As a result, the following threats have been identified:

T.UnwantedManagementTraffic The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exists on the management plane. The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations. As a consequence, the TOE might be unable to provide some of the TSF while under attack and in particular security management functionality to update configuration data for the TOE. Subsequently, backup of audit information before local storage space is exceeded and old audit information is overwritten by new audit events could be affected. Therefore, Audit data and Configuration data for the TOE are assets that could be affected by this threat, too.

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. This could affect all assets as defined in chap. 3.1 .

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. This could affect all assets as defined in chap. 3.1 .

T.Intercept A remote attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and EMS. This comprises Auth data (in particular authentication data of administrative users), Crypto data (regarding this threat mainly data related to session keys used for secure communication), and Configuration Data for the TOE. All these assets could be affected by this threat.

3.3 Organizational Security Policies

This section specifies one organizational security policy (OSP) to be met by the TOE and the TOE environment.

OSP.Accountability The users of the TOE shall be held accountable for their security-relevant actions within the TOE.

3.4 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

A.Certificates It is assumed that digital certificates that are generated externally by trusted certification authorities are of good quality i.e. meeting corresponding standards and providing sufficient security strength through the use of appropriate cryptographic mechanisms and cryptographic parameters. This applies for the cryptographic mechanisms and parameters contained in the certificate and as well for the mechanisms and parameters used to sign the certificate. It is assumed that administrators examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms are assumed to be not imported into the TOE.

A.PhysicalProtection It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals, such as a board, and CF card inserted in the transmission equipment) are protected against unauthorized physical access. It is also assumed that the local management network, including the RADIUS server, syslog server, and locally attached management terminals (LMT) together with all related communication lines are operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) need to be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physical protection. It is assumed that all RMTs as well as peripherals like RADIUS server or syslog server are connected to the TOE via the same segregated management network (see also A.NetworkSegregation).

A.NetworkElements It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. This applies e.g. to the EMS used for TOE management, Syslog servers, SFTP servers and Radius servers for obtaining authentication and authorization decisions.

A.NetworkSegregation It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.

A.NoEvil It is assumed that personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative 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.

A.Time It is assumed that external clock used by the NTP client is reliable.

A.Hardware It is assumed that the underlying hardware of OptiX OSN 1800 V, which is outside the scope of the TOE, works correctly.

A.RNG It is assumed that the TPM, which provides the seed to the RNG, is reliable and therefore provides a seed value of sufficient entropy.

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O.DataFilter** The TOE shall ensure that only allowed management traffic goes through the TOE.
- **O.Authorization** The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.
- **O.Authentication** The TOE must authenticate users before access to data and security functions is granted.
- **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.
- **O.SecurityManagement** The TOE shall provide functionality to manage security functions provided by the TOE.

4.2 Security Objectives for the Operational Environment

- **OE.Certificates** Digital certificates that are generated externally by trusted certification authorities shall be of good quality i.e. meeting corresponding standards and providing sufficient security strength through the use of appropriate cryptographic mechanisms and cryptographic parameters. This applies for the cryptographic mechanisms and parameters contained in the certificate and as well for the mechanisms and parameters used to sign the certificate. Administrators shall examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms shall not be imported into the TOE.
- **OE.PhysicalProtection** The TOE and its operational environment (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. The local management network, including the RADIUS server, syslog server, and locally attached management terminals (LMT) together with all related communication lines shall be operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) shall be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic

means and do not need any physically protection. All RMTs as well as peripherals like RADIUS server or syslog server shall be connected to the TOE via the same segregated management network (see also OE.NetworkSegregation).

- **OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behavior of such network devices provided by the operational environment shall be secure and correct. This applies e.g. to EMS used for TOE management, Syslog servers, SFTP servers and Radius servers for obtaining authentication and authorization decisions.
- **OE.NetworkSegregation** The operational environment shall provide segregation of networks by deploying the management interface in TOE into an independent local network.
- **OE.NoEvil** Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or willfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation.
- **OE.Time** The external clock used by the NTP client shall be reliable.
- **OE.Hardware** The underlying hardware of OptiX OSN 1800 V, which is outside the scope of the TOE, shall work correctly.
- **OE.RNG** The TPM, which provides the seed to the RNG, shall be reliable and therefore provides a seed value of sufficient entropy.

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 and OSPs

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.UnwantedManagementTraffic	O.DataFilter O.SecurityManagement	This threat is countered by O.DataFilter ensuring that unwanted traffic is filtered and cannot deplete the network resources. The filter rules can be configured by authorized users with sufficient user level (O.SecurityManagement).
T.UnauthenticatedAccess	O.Authentication O.Audit O.SecurityManagement	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.UnauthorizedAccess	O.Authorization O.Audit O.SecurityManagement	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). Access control mechanisms (including user levels) can be configured by users with sufficient user level (O.SecurityManagement). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit).
T. Intercept	O.Communication O.SecurityManagement	The threat of eavesdropping is countered by requiring communications security via TLS and SFTP for communication between EMS and the TOE (O.Communication). Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement).
OSP.Accountability	O.Authentication O.Audit	Accountability for security-relevant actions is achieved by generating audit records for those events (O.Audit). Attributing security-relevant events to their originators requires users to be properly identified and authenticated (O.Authentication)

The following table provides a mapping of the objectives for the operational environment to assumptions, showing that each objective is covered exactly by one assumption. The objectives for the environment are mirrored by the assumptions. Therefore, the mapping is trivial.

A. Certificates is upheld by OE.Certificates, which is a rephrasing of the assumption.

A. PhysicalProtection is upheld by OE.PhysicalProtection, which is a rephrasing of the assumption.

A.NetworkElements is upheld by OE.NetworkElements, which is a rephrasing of the assumption.

A.NetworkSegregation is upheld by OE.NetworkSegregation, which is a rephrasing of the assumption.

A.NoEvil is upheld by OE.NoEvil, which is a rephrasing of the assumption.

A.Hardware is upheld by OE.Hardware, which is a rephrasing of the assumption.

A.Time is upheld by OE.Time, which is a rephrasing of the assumption.

A.RNG is upheld by OE.RNG, which is a rephrasing of the assumption.

Table 4-2 Mapping objectives for the environment to assumptions

Environmental Objective	Threat /Assumption
OE.Certificates	A.Certificates
OE.PhysicalProtection	A.PhysicalProtection
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation
OE.NoEvil	A.NoEvil
OE.Hardware	A.Hardware
OE.Time	A.Time
OE.RNG	A.RNG

5 Extended Components Definition

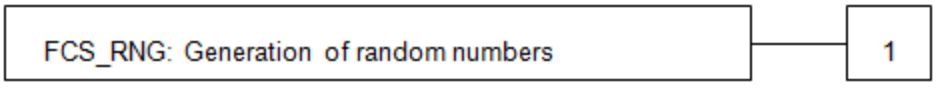
There is one extended component defined which refers to random number generation and is taken from chap. 3.1 [AIS20].

5.1 FCS_RNG Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:



FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

6 Security Requirements for the TOE

6.1 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.
- Iteration/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 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:

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

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

c) **The following auditable events recorded to operation logs:**

i. user activity

1. **login, logout**
2. **system and service configuration operation requests (i.e. configuration of the device after start-up)**
3. **system security configuration.**

The following auditable events recorded to security logs:

ii. user management

1. **add, delete, modify users**
2. **user password change**
3. **user group level change**
4. **user lock and unlock**

Application Note: Changes to user levels are covered by c.ii.3. user group level change. Command levels are fixed and cannot be modified. Audit functionality shall be enabled by default during start-up of the device. The audit functionality cannot be shut down manually. The audit functionality can only be shut down by shutdown of the OptiX OSN 1800 V itself. In that case there is only an audit record generated for the shutdown of the device but not the audit functionality in particular.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **Operation Type (if applicable)**, **Operation Object (if applicable), Access IP Address (if applicable)**, **User Name (if applicable).**

Application Note: The term 'if applicable' shall be read as 'whenever an event can be associated with the specified information'. For example, if an event can be associated with a User ID, then the event shall be audited and the audit information shall contain the User ID. If the event cannot be associated with the User ID, the event shall be audited and the audit information shall not contain User ID information. If multiple conditional information can be associated with an event (e.g. interface and User ID can be associated with an event), all the conditional information shall be contained in the audit information when auditing the event.

6.2.1.2 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.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **Administrators and Super administrators** 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.

6.2.1.4 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.

6.2.1.5 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.

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

FAU_STG.3.1 The TSF shall **overwrite the oldest records** if the audit trail exceeds **the size of the storage device**.

Application Note: The audit trail is recorded in log file on the storage media (FLASH), the size of log file is fixed.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1/DH Cryptographic key generation

FCS_CKM.1.1/DH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **diffie-hellman-group14-sha1** and specified cryptographic key sizes **2048bits** that meet the following: **[NIST Special Publication 800-56A], [RFC 4253], [RFC 3526], [RFC 4346], [RFC 5246], [PKCS#3] for SSH/TLS.**

Application Note: When establish SSH/TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption, and generation and verification of integrity protection information for SSH/TLS communication. The key generation is performed according to [RFC 4253].

6.2.2.2 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **2048 bits to 4096 bits** that meet the following: **[FIPS 186-4], chap. 5.1, RSA key pairs for RSASSA-PKCS1-V1_5 using CRT, chap. 6.3.**

Application Note: The RSA Key Pair generation algorithm meets [FIPS 186-4], chap. 5.1 and adapts method in Appendix B.3.3. The TOE uses RSA keygen method to generate ‘SSH host key’ which is used as client key within the SFTP protocol.

6.2.2.3 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method:

- **diffie-hellman-group14-sha1** that meets the following: **[NIST Special Publication 800-56A], [RFC 4253], [RFC 3526], [RFC 4346], [RFC 5246], [PKCS#3] for SSH and TLS.**
- **RSA-based key establishment scheme that meets the following: [NIST SP 800-56B] for TLS.**

Application Note: When establish SSH/TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement or RSA key exchange. The shared secret value is used to derive session keys used for encryption and decryption, and generation and verification of integrity protection information for SSH/TLS communication. The key generation is performed according to [RFC 4253].

6.2.2.4 FCS_CKM.4/DH Cryptographic key destruction

FCS_CKM.4.1/DH The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **deallocation of the resource** that meets the following: **none.**

Application Note: Whenever a Trusted Channel is terminated for whatever reason, all temporary session keys are erased from the volatile memory by the post-processing routines associated with the Trusted Channel. These session keys are generated by FCS_CKM.1/DH

6.2.2.5 FCS_CKM.4/RSA Cryptographic key destruction

FCS_CKM.4.1/RSA The TSF shall destroy cryptographic (RSA) keys in accordance with a specified cryptographic key destruction method **full flash erase by overwriting with 1** that meets the following: **none**

Application Note: This SFR was refined to RSA keys in the non-volatile memory only. The RSA Keys will be stored in flash memory of the SCC board. The private key cannot be exported. OptiX OSN1800V provides a manual method to erase all the data on flash at a time (i.e. full flash erase by overwriting the whole flash memory with '1'). All the data in the flash memory including RSA Keys and the configuration DB will be erased, and the equipment returns to the factory reset status.

According to A.PhysicalProtection, the OptiX OSN1800V device is deployed in a secured environment. Therefore, the key destruction mechanism for RSA keys in non-volatile memory is intended to be used when the TOE is leaving the secured area (e.g. when decommissioned) to destroy residual information. There is no destruction mechanism to selectively destroy RSA keys during regular use of the TOE.

6.2.2.6 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1/AES The TSF shall perform **symmetric de- and encryption** in accordance with a specified cryptographic algorithm **AES,** with operating modes, keysizes and underlying standards as defined in the following table.

Table 6-1 AES operating modes supported by the TOE for symmetric de- and encryption

AES operating mode	Cryptographic key sizes [bits]	Meeting the standards
GCM mode	128, 256	[FIPS 197], [NIST SP 800-38D]
CTR mode	128, 192, 256	[FIPS 197], [NIST SP 800-38A]
CBC mode	128, 256	[FIPS 197], [NIST SP 800-38A]

Application Note: AES-128, 192, 256 in CTR mode is used for encryption and decryption within SSH communication. AES-128/256 in CBC mode is not supported within SSH communication.

AES-128/256 in GCM mode is used for encryption and decryption within TLS communication.

AES-128/256 in CBC mode is used for encryption and decryption within TLS communication.

6.2.2.7 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1/RSA The TSF shall perform **asymmetric authentication** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 to 4096bits** that meet the following: **RSA Cryptography Standard ([PKCS#1 V2.1], RSASSA-PKCS1-v1_5 for SSH and TLS).**

Application Note: RSA with key size of 2048 to 4096bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 is used for asymmetric authentication of the TOE (as SFTP client) for SSH according to chap. 6.6 [RFC 4253], ssh-rsa as well as 'publickey' authentication of the TOE (as SFTP client) to the server for SSH according to chap. 7 [RFC 4252].

RSA with key size of 2048 to 4096bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 is used for asymmetric authentication of TLS. (TLS cipher suites refer to 6.2.8.1)

Certificates used by TLS are imported by users into the TOE. Therefore, the TOE does not provide path validation capabilities for X.509 certificates. It is assumed that the weak RSA key (size less than 2048 bits) and hashing algorithms will not to be imported into the TOE. If the hashing algorithms specified in the certificates are not supported by the TOE, the TLS communication will not be established successfully.

6.2.2.8 FCS_COP.1/HMAC-SHA1 Cryptographic operation

FCS_COP.1.1/HMAC-SHA1 The TSF shall perform **data integrity generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA1** and cryptographic key sizes **160 bits** that meet the following: [**RFC 2104], [FIPS 198-1].**

Application Note: HMAC-SHA1 is used for integrity protection of SSH communication.

6.2.2.9 FCS_COP.1/HMAC-SHA1-96 Cryptographic operation

FCS_COP.1.1/HMAC_SHA1-96 The TSF shall perform **data integrity generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA1-96** and cryptographic key sizes **160 bits** that meet the following: [**RFC 2104], [FIPS 198-1].**

Application Note: HMAC-SHA1-96 is used for integrity protection of SSH communication. HMAC-SHA1-96 is cryptographic key sizes of 160 bit that is truncated to 96 bit.

6.2.2.10 FCS_COP.1/HMAC-SHA256 Cryptographic operation

FCS_COP.1.1/HMAC-SHA256 The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA256** and cryptographic key sizes **256bits** that meet the following: [**RFC 2104], [FIPS 180-4].**

Application Note: HMAC-SHA256 is used in the TLS communication according to [RFC 4346] and [RFC 5246].

6.2.2.11 FCS_COP.1/HMAC-SHA384 Cryptographic operation

FCS_COP.1.1/HMAC-SHA384 The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA384** and cryptographic key sizes **384bits** that meet the following: [**RFC 2104], [FIPS 180-4].**

Application Note: HMAC-SHA384 is used in the TLS communication according to [RFC 4346] and [RFC 5246].

6.2.2.12 FCS_COP.1/SHA1 Cryptographic operation

FCS_COP.1.1/SHA1 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA1** and cryptographic key sizes **None** that meet the following: **[FIPS 180-3].**

Application Note: SHA1 is used for hashing within SSH communication.

6.2.2.13 FCS_COP.1/SHA256 Cryptographic operation

FCS_COP.1.1/SHA256 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA256** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA256 is used in TLS communication.

6.2.2.14 FCS_COP.1/SHA384 Cryptographic operation

FCS_COP.1.1/SHA384 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA384** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA384 is used in TLS communication.

6.2.2.15 FCS_COP.1/PBKDF2 Cryptographic operation

FCS_COP.1.1/PBKDF2 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **PBKDF2(HMAC-SHA256) with iteration number 10000** and cryptographic key sizes **None** that meet the following: **[RFC2898].**

Application Note: PBKDF2 is used for hashing passwords before storage in non-volatile memory. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE's deterministic random number generator.

6.2.2.16 FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1 The TSF shall provide a ***deterministic*** random number generator that implements:

- **DRG.3.1: If initialized with a random seed of 32 bytes that shall contain at least 128 bit entropy the internal state of the RNG shall have Min-entropy of at least 100 bits.**
- **DRG.3.2: The DRNG provides forward secrecy.**
- **DRG.3.3: The DRNG provides backward secrecy even if the current internal state is known.**

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

- **DRG.3.4: The RNG, initialized with a random seed of 256 bits during the preparative operations ensured by the preparative procedures for users generates output for which more than 2^{14} strings of bit length 128 are mutually different with probability greater than $1-2^{-8}$.**
- **DRG.3.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A and no other test suites.**

Application Note: The operations have been performed according to chap. 4.8 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bits entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The TOE will seed the DRNG at the module initialization stage before start of TLS-based communication and SSH-based communication.

The DRNG complies with [NIST SP 800-90A] using HMAC-DRBG (SHA-256).

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **user group SFP** on

Subject: user session;

Objects: commands provided by TOE;

Operation: Execute

6.2.3.2 FDP_ACF.1 Security Attribute based Access Control

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

Subject security attributes

users and their following security attributes:

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

Objects security attributes:

commands and their following security attributes:

- **Commands and command level (There are five command levels: Monitor, Operate, Maintain, Manage, Debug)**

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.**
2. **Users can be configured with different user group to control the device access permission.**
3. **There are five user groups: Monitor, Operator, Maintainer, Administrator, Super administrator, in ascending order of privilege level.**
4. **Each user group corresponds to different command levels. A user can run all commands from the command level corresponding to his user level (see table 7-1) and below.**
5. **The command level is defined by the software and cannot be changed.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

6.2.3.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the Management Network Traffic Flow Filtering SFP on

Subjects:

packets from the management network

Information:

Package content (management data);

Operations:

Permit, Deny the incoming of packets from the management network based on information security attributes as defined in chap. 6.2.3.4.

6.2.3.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **Management Network Traffic Flow Filtering SFP** based on the following types of subject and information security attributes

Subject: packets from the management network

Subject attributes: Source IP address, Destination IP address, protocol type, Source tcp or udp port number, Destination tcp or udp port number

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:

1. **Whenever an incoming management network packet is handled by TCPIP protocol layer 3 (forwarding or accepting) on TOE, the Access Control List (ACL) will be checked.**
2. **The ACL rules could either permit or deny forwarding or accepting based on the information security attributes 'source IP address', 'destination IP address', 'protocol type', 'source tcp or udp port number', 'destination tcp or udp port number'. Rules have to contain at least one of the attributes but may contain several attributes.**
3. **For every incoming management network packet that is intended to be forwarded or accepted by the TOE the ACL is checked for a rule that matches the attributes of the packet, respectively starting from the first entry in the ACL. The ACL is checked until the first matching rule is found. The network packet is then either passed (forwarded/accepted) or discarded according to the matching rule in the ACL. If no matching rule is found, the packet is passed.**

FDP_IFF.1.3 The TSF shall enforce the **no additional information flow control SFP rules**.

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: **none.**

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **5** (consecutive) 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. lock the offending user ID;

2. audit the event in the security log.

Application Note: The default value for the maximum number of consecutive failed logins is five.

6.2.4.2 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 validity period

3. user level

4. password

5. password validity period

6. the inactivity time after which an account is automatically logged out.

7. Status of the account (locked/unlocked)

8. number of failed consecutive logins within certain period of time and timestamp of last successful login

6.2.4.3 FIA_UAU.2 User authentication before any action

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

Application Note: Authentication is possible by username and password.

6.2.4.4 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 users based on the configured Identification (including user id and password).

Application Note: The TOE can use only one of the mechanisms at any given time. The Administrator can configure which mechanism is used by the TOE.

6.2.4.5 FIA_UID.2 User identification before any action

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

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

6.2.4.6 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **User ID**
- **User level**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **None**.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **None**.

Application Note: The TOE subjects of relevance are management sessions and SFTP sessions.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***determine the behavior of*** the functions **defined in FMT_SMF.1** to **users with sufficient user level as defined in FMT_SMR.1**.

6.2.5.2 FMT_MSA.1/ACFATD Management of Security Attributes (user group SFP)

FMT_MSA.1.1/ACFATD The TSF shall enforce the **user group SFP** to restrict the ability to ***query, modify*** the security attributes **NTP server address, SYSLOG server address, RADIUS server address, SFTP server address, and Attributes identified in FDP_ACF.1 and FIA_ATD.1** to **the users with sufficient user level as defined in FMT_SMR.1**.

6.2.5.3 FMT_MSA.1/IFF Management of Security Attributes

FMT_MSA.1.1/IFF The TSF shall enforce the **Management Network Filtering SFP** to restrict the ability to ***delete, modify*** the **security attributes identified in FDP_IFF.1** to **users with sufficient user level as defined in FMT_SMR.1**

6.2.5.4 FMT_MSA.3/ACFATD Static Attribute Initialization

FMT_MSA.3.1/ACFATD The TSF shall enforce the **user group SFP** to provide ***permissive*** default values for security attributes (User Group associations) that are used to enforce the SFP.

FMT_MSA.3.2/ACFATD The TSF shall allow **users with sufficient user level as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_MSA.3/IFF Static Attribute Initialization

FMT_MSA.3.1/IFF The TSF shall enforce the **Management Network Filtering SFP (based on ACL)** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IFF The TSF shall allow **users with sufficient user level as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

6.2.5.6 FMT_SMF.1 Specification of Management Functions

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

1. **Management of user accounts and user attributes, including user credentials**
2. **Management of authentication failure policy**
3. **Management of ACLs and ACL parameters like IP addresses or address ranges**
4. **Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP**
5. **Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces**
6. **Management of the TOE's time**

6.2.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. **Monitor (as defined in the table below)**
2. **Operator (as defined in the table below)**
3. **Maintenance (as defined in the table below)**
4. **Administrator (as defined in the table below)**
5. **Super administrator (as defined in the table below)**

Role	Authority
Monitor	This group has the lowest authority. The accounts of this group are authorized to issue query commands and modify some of their own attributes.
Operator	The accounts of this group are authorized to query the system information and perform some configuration operations.

Role	Authority
Maintenance	The accounts of this group are authorized to perform all maintenance operations, including the authority of Operator group and general maintenance and diagnosis operations
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations. Especially, administrators can create super administrator account.
Super administrator	The accounts in this group are authorized to perform all operations of Administrator group and the advanced diagnosis (debug) operation.

Application Note: The roles are hierarchical, i.e. each role includes all authorities of the previous roles in addition to the authorities described for the role itself.

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable Timestamps

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

6.2.7 TOE access (FTA)

6.2.7.1 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.**

6.2.7.2 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

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_ITC.1/TLS Inter-TSF trusted channel

FTP_ITC.1.1/TLS The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

Application Note: To establish a trusted channel, the TLS protocol shall be used. TLS complies with RFC 5246 (TLS1.2), and RFC 4346 (TLS1.1).

The following cipher suites for TLS-based communication are supported by the TOE:

- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246
- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268

Client authentication is performed password-based on the application layer.

FTP_ITC.1.2/TLS The TSF shall permit ***another trusted IT product*** to initiate communication via the trusted channel.

Application Note: The EMS will act as TLS client to initiate communication to the TOE which acts as TLS server.

FTP_ITC.1.3/TLS The TSF shall initiate communication via the trusted channel for **none**.

Application Note: The TSF do not initiate any TLS-based communication, but offers the ability for protected communication for users sessions.

6.2.8.2 FTP_ITC.1/SFTP Inter-TSF trusted channel

FTP_ITC.1.1/SFTP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2/SFTP The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1.3/SFTP The TSF shall initiate communication via the trusted channel for **file transfer via SFTP**.

Application Note: To establish a trusted channel, the SSH(SFTP) protocol shall be used. SFTP complies with [RFC 4251], [RFC 4252], [RFC 4253], and [RFC 4254].

For SSH/SFTP-based communications the following algorithms and ciphers are supported:

- Authentication can be performed either public key-based or password-based as described in [RFC 4252].
- Key exchange is performed using diffie-hellman-group 14-sha1
- The public key algorithm of the SSH transport implementation is ssh-rsa.

- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC-SHA1, HMAC-SHA1-96 are supported.

6.3 Security Functional Requirements Rationale

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 6-2 Mapping SFRs to objectives

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_STG.1	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1/AES FCS_COP.1/RSA FCS_COP.1/HMAC-SHA1 FCS_COP.1/HMAC-SHA1-96 FCS_COP.1/HMAC-SHA256 FCS_COP.1/HMAC-SHA384 FCS_COP.1/SHA256 FCS_COP.1/SHA384 FCS_COP.1/SHA1	O.Communication
FCS_COP.1/PBKDF2	O.Authentication, O.Communication
FCS_CKM.1/DH FCS_CKM.1/RSA	O.Communication
FCS_CKM.2	O.Communication
FCS_CKM.4/DH FCS_CKM.4/RSA	O.Communication
FCS_RNG.1	O.Communication
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FDP_IFC.1	O.DataFilter

FDP_IFF.1	O.DataFilter
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_UAU.2	O.Authentication
FIA_UAU.5	O.Authentication
FIA_UID.2	O.Authentication O.Authorization
FIA_USB.1	O.Authentication O.Authorization
FMT_MOF.1	O.Authorization O.SecurityManagement
FMT_MSA.1/ACFATD	O.Authorization O.SecurityManagement
FMT_MSA.1/IFF	O.Authorization O.DataFilter O.SecurityManagement
FMT_MSA.3/ACFATD	O.Authorization O.SecurityManagement
FMT_MSA.3/IFF	O.Authorization O.DataFilter O.SecurityManagement
FMT_SMF.1	O.SecurityManagement O.DataFilter
FMT_SMR.1	O.Authorization O.SecurityManagement
FPT_STM.1	O.Audit
FTA_SSL.3	O.Authentication
FTA_TSE.1	O.DataFilter O.Authentication
FTP_ITC.1/TLS	O.Authentication O.Communication
FTP_ITC.1/SFTP	O.Authentication O.Communication

6.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Table 6-3 SFR sufficiency analysis

Security objective	Rationale
O.DataFilter	The requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF and FMT_SMF.1. Rejection of connections is addressed by FTA_TSE.1.
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable. User identities are available through binding management sessions to their users (FIA_USB.1). Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.2. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the audit trail exceeds the size of the storage device The TSF shall roll back the oldest records as required by FAU_STG.3.
O.Communication	Communication security is implemented by the establishment of a trusted channel for remote users in FTP_ITC.1/TLS and FTP_ITC.1/SFTP. FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA1-96, FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384, FCS_COP.1/SHA256, FCS_COP.1/SHA384 and FCS_COP.1/SHA1 are providing the cryptographic functions required for TLS and SFTP channels. Password-based user authentication requires password hashing provided by FCS_COP.1/PBKDF2. FCS_CKM.1/RSA, and FCS_CKM.1/DH addresses key generation of AES/RSA keys. FCS_CKM.2 addresses distribution of session keys for AES keys and the RSA key exchange. FCS_CKM.4/RSA addresses key destruction of RSA keys. Note that keys of AES algorithms as a result of the DH key agreement are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination according to FCS_CKM.4/DH. The allocated memory is freed as well. Random numbers needed for secure communication are addressed by FCS_RNG.1.

O.Authentication	User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. Remote user authentication by RADIUS as well as authentication via local database is implemented by FIA_UAU.5. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1 and the subjects acting on the behalf of that user are addressed in FIA_USB.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1. For password verification hash values of passwords are used which are generated using FCS_COP.1/PBKDF2. User authentication via RMTs requires the use of a trusted path according to FTP_ITC.1/TLS and FTP_ITC.1/SFTP. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.
O.Authorization	User identification is addressed in FIA_UID.2. User IDs and user levels are bound to management sessions and available for access control decisions through user-subject binding (FIA_USB.1). The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. User-related attributes are spelled out in FIA_ATD.1 and the subjects acting on the behalf of that user are spelled out in FIA_USB.1 Security Management is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1 and FMT_MOF.1. Requirements on the management functionality for the definition of access control policies and other security functions behavior, security attributes, and static attribute initialization are provided in FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ ACFATD, and FMT_MSA.3/IFF.
O.Security Management	The requirements on management of security functions behavior, security attributes, and static attribute initialization are provided in FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, and FMT_SMF.1. The management functionality for the security functions of the TOE is defined in FMT_SMF.1 and the security user roles are defined in FMT_SMR.1.

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 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 6-4 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.2
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
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	TLS/SFTP: FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	SFTP: FCS_CKM.1/RSA FCS_CKM.4/RSA TLS: Unsupported: FCS_CKM.1; FCS_CKM.4
FCS_COP.1/HMAC-SHA1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/HMAC-SHA1-96	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/HMAC-SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/HMAC-SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/SHA1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4

Security Functional Requirement	Dependency	Resolution
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_CKM.1/DH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_CKM.2 FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA1-96 FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384 FCS_CKM.4/DH
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA FCS_CKM.4/RSA
FCS_CKM.2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_CKM.4/DH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/DH
FCS_CKM.4/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA
FCS_RNG.1	No Dependencies	None
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_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3

Security Functional Requirement	Dependency	Resolution
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No Dependencies	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	No Dependencies	None
FIA_UID.2	No Dependencies	None
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/ACFATD	[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.1/IFF	[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/ACFATD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ACFATD FMT_SMR.1
FMT_MSA.3/IFF	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/IFF FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	No Dependencies	None
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_ITC.1/TLS	No Dependencies	None
FTP_ITC.1/SFTP	No Dependencies	None

6.3.4 Justification for unsupported dependencies

The following dependencies are unsupported for the reasons given below.

FCS_COP.1/SHA1, FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/PBKDF2: Hash functions do not require keys, so FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, and FCS_CKM.4 are not applicable.

FCS_CKM.1/RSA: The key of RSA in TLS is obtained from the TLS certificate, so FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, and FCS_CKM.4 are not applicable.

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2, as specified in [CC] Part 3. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL2) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

7 TOE Summary Specification

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

7.1 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. The pre-defined user information (reference data) is the user password hashed using the PBKDF2 (HMAC-SHA256) function as defined in the 'Cryptographic Functions' TOE Security Function. Passwords have a length of 16 characters. The TOE enforces a password complexity policy of at least contains three types of the following character types: capital letter, small letter, number, and special character.
- Support authentication via the remote RADIUS authentication server. The TOE hands identification and authentication information provided by the user during login to the RADIUS server and enforces the RADIUS server’s pass/fail decision.
- Support authenticated user logins using the TLS 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 TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login. By default, the inactivity period is 60 minutes.
- Support maximum attempts for authentication failures within certain period of time. By default, after five consecutive 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. The default value of lock period is 15 minutes, the configurable range is between 1 and 1000 minutes. So the user account will be automatically unlocked after 15 minutes by default.
- Support access limit by IP-based ACL. A series of whitelists and blacklists are set to filter IP addresses and data on 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.
- Using the SFTP application requires Administrator users to unlock the private RSA key for SFTP first with the key’s passphrase. When the key is generated, the Administrator is

allowed to set a passphrase of 12 to 16 characters. The passphrase complexity requirements are the same as for user passwords.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FIA_USB.1, FCS_COP.1/PBKDF2, FTA_TSE.1, FTA_SSL.3)

Table 7-1 SFR to TSF mapping

SFR	TSF
FIA_AFL.1	Support maximum attempts for authentication failures within certain period of time. By default, after five consecutive 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.
FIA_ATD.1 FIA_USB.1	Support authentication via local passwords. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Passwords have a length of 16 characters. The TOE enforces a password complexity policy of at least contains three types of the following character types: capital letter, small letter, number, and special character. 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 TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login. By default, the inactivity period is 60 minutes. Support maximum attempts for authentication failures within certain period of time. By default, after five consecutive 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. Using the SFTP application requires Administrator users to unlock the private RSA key for SFTP first with the key's passphrase. When the key is generated, the Administrator must set a passphrase of 12 to 16 characters. The passphrase complexity requirements are the same as for user passwords. Support for user individual attributes including the user ID, user level, and password to ensure that each user is unique in the system.
FIA_UAU.2	The TOE enforces that every user needs to successfully authenticate himself by username and password before he can use any TOE security function other than the identification and authentication function. The TOE provides two session establishment mechanisms requiring identification and authentication of users: via MML commands for file uploads and downloads over SFTP and via QX commands for all other administrative

	activities.
FIA_UAU.5	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. The TOE hands identification and authentication information provided by the user during login to the RADIUS server and enforces the RADIUS server's pass/fail decision.
FIA_UID.2	The TOE enforces that every user is successfully identified by username when providing username and password for authentication before he can use any TOE security function other than the identification and authentication function.
FCS_COP.1/PBKDF2	The pre-defined user information (reference data) is the user password hashed using the PBKDF2 (HMAC-SHA256) function as defined in the 'Cryptographic Functions' TOE Security Function.
FTA_TSE.1	Support access limit by IP-based ACL. A series of whitelists and blacklists are set to filter IP addresses and data on ports. Unauthorized IP addresses and communication ports cannot access the system. Support authenticated user logins using the TLS mode.
FTA_SSL.3	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 TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login. By default, the inactivity period is 60 minutes.

7.2 Authorization

The TOE enforces an access control by supporting following functions:

- There are five hierarchical user groups (from low to high): monitor, operator, maintenance, administrator and super administrator.
- A user group is assigned to each account.
- Accounts are managed in groups. 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 audited. The authority of each user group is specified in table 1-2.
- Every management command has a *command level* associated to it. A user can use this command if his user level dominates the command level, i.e., if his user level is hierarchically equal or higher than the command level. User groups match to command levels as follows:

Table 7-2 Correspondence of user groups and command levels

User group	Command Level
Monitor	Monitor
Operate	Monitor Operate
Maintenance	Monitor Operate Maintenance
Administrator	Monitor Operate Maintenance Manage
Super Administrator	Monitor Operate Maintenance Manage Debug

- In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user level attribute beyond their own user level. Command levels cannot be changed by users.
- Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging commands. Only Administrators and Super administrators can query and dump operation logs and security logs.

(FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, FMT_SMF.1, FMT_SMR.1)

Table 7-3 SFR to TSF mapping

SFR	**TSF**
FDP_ACC.1	Accounts are managed in groups. 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 audited. The authority of each user group is specified in table 1-2. In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user level attribute beyond their own user level. Command levels cannot be changed by users.

FDP_ACF.1	There are five hierarchical user groups (from low to high): monitor, operator, maintenance, administrator and super administrator. A user group is assigned to each account. Accounts are managed in groups. 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 audited. The authority of each user group is specified in table 1-2. Every management command has a command level associated to it. A user can use this command if his user level dominates the command level, i.e., if his user level is hierarchically equal or higher than the command level. User groups match to command levels as follows: Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging commands. Only Administrators and Super administrators can query and dump operation logs and security logs.
FMT_MOF.1	Accounts are managed in groups. 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 audited. The authority of each user group is specified in table 1-2. Every management command has a command level associated to it. A user can use this command if his user level dominates the command level, i.e., if his user level is hierarchically equal or higher than the command level. User groups match to command levels as follows: Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging commands. Only Administrators and Super administrators can query and dump operation logs and security logs.
FMT_MSA.1/ACFATD FMT_MSA.1/IFF FMT_MSA.3/ACFATD FMT_MSA.3/IFF FMT_SMF.1	Accounts are managed in groups. 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 audited. The authority of each user group is specified in table 1-2. Every management command has a command level associated to it. A user can use this command if his user level dominates the command level, i.e., if his user level is

	hierarchically equal or higher than the command level. User groups match to command levels as follows: Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging commands. Only Administrators and Super administrators can query and dump operation logs and security logs.
FMT_SMR.1	There are five hierarchical user groups (from low to high): monitor, operator, maintenance, administrator and super administrator. A user group is assigned to each account. Both administrator and super administrator accounts belong to the administrator level and both have the privilege to create other administrator or super administrator accounts. The super administrator is a special administrator (expert role for equipment diagnoses and maintenance) that can execute the debugging commands. Only Administrators and Super administrators can query and dump operation logs and security logs.

7.3 Auditing

The TOE provides an audit trail consisting of operation logs and security logs:

- Support recording non-query operations in the operation logs, including the operation type (if applicable), operation object (if applicable), access IP address (if applicable), date and time, the outcome, and user name (if applicable).
- 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, date and time, operation, and outcome.
- For all audit events the corresponding timestamp will be recorded together with the event.
- Only Administrators and Super administrators can query and dump operation logs and security logs, and the Administrators and Super administrators can know that whoever accesses and logins the system and any operation on the system according to the content of the security log and the operation log.
- The operation logs and security logs allow no manual changes.
- The operation logs and security logs can be completely recovered even after a power-outage restart of the system.
- The operation logs and security logs keep records in time sequence. After the memory is exhausted, the earliest records of the logs are overwritten by the latest records. Once the memory is exhausted, a performance event is reported.

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

Table 7-4 SFR to TSF mapping

SFR	TSF
FAU_GEN.1	Support recording non-query operations in the operation logs, including the operation type, operation object, access IP address, date and time, the outcome, and 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, date and time, operation, and outcome. For all audit events the corresponding timestamp will be recorded together with the event.
FAU_GEN.2	Support recording non-query operations in the operation logs, including the operation type, operation object, access IP address, date and time, the outcome, and user name.
FAU_SAR.1 FAU_SAR.2	Only Administrators and Super administrators can query and dump operation logs and security logs. So only the Administrators and Super administrators can know that whoever accesses and logins the system and any operation on the system according to the content of the security log and the operation log.
FAU_STG.1	The operation logs and security logs allow no manual changes.
FAU_STG.3	The operation logs and security logs can be completely recovered even after a power-outage restart of the system. The operation logs and security logs keep records in time sequence. After the memory is exhausted, the earliest records of the logs are overwritten by the latest records. Once the memory is exhausted, a performance event is reported.

7.4 Communication Security

The TOE provides communication security by implementing trusted channels between the EMS and the TOE using the TLS communication protocol. The TLS1.1 and TLS1.2 protocols are implemented to provide communication channels. The TOE acts as a TLS server and allows other trusted IT products to initiate communication. The TLS certificates for server authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. Client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery. If the below-mentioned TLS_RSA ciphers are used, the RSA public key is used for authentication and key exchange. Using the below TLS_DHE ciphers the standard Diffie-Hellman parameters P and G.

The following TLS ciphers are supported by the TOE, for details of the ciphers, please refer to chapter 7.8:

- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246
- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268

The TOE provides communication security by establishing a trusted channel for secure file transfer based on the SSH(SFTP) protocol. The TOE acts as a SFTP client which initiates communication with other trusted IT products. The SSH/SFTP-based communication is based on the following algorithms and ciphers, for details of the cipher, please refer to chapter 7.8:

- Authentication can be performed either public key-based or password-based as described in RFC 4252.
- Key exchange is performed using diffie-hellman-group 14-sha1
- The public key algorithm of the SSH transport implementation is ssh-rsa.
- For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported.
- For data integrity protection HMAC-SHA1, HMAC-SHA1-96 are supported.

The TOE supports session time-out after a configurable time of user inactivity. After the session has expired, the equipment user account will be automatically logged out.

The TOE supports denying session establishment based on authentication failure (i.e. device authentication failure for TLS and user authentication as well as device authentication failure for SFTP).

The TOE supports denying session establishment based on source IP address with is based on the ACL mechanisms of the Management Traffic Flow Control TOE Security Function.

(FTA_TSE.1, FTP_ITC.1/TLS, FTP_ITC.1/SFTP)

Table 7-5 SFR to TSF mapping

SFR	TSF
FTP_ITC.1/TLS	The TOE provides communication security by implementing trusted channels between the EMS and the TOE using the TLS communication protocol. The TLS1.1 and TLS1.2 protocols are implemented to provide communication channels. The TOE acts as a TLS server and allows other trusted IT products to initiate

	communication. The TLS certificates for server authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. Client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery. The following TLS ciphers are supported by the TOE, for details of the cipher, please refer to chapter 7.8: TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288 TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246 TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5246 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246 TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268 TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC3268 TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC3268
FTP_ITC.1/SFTP	The TOE provides communication security by establishing a trusted channel for secure file transfer based on the SSH(SFTP) protocol. The TOE acts as a SFTP client which initiates communication with other trusted IT products. The SSH/SFTP-based communication is based on the following algorithms and ciphers, for details of the cipher, please refer to chapter 7.8: Authentication can be performed either public key-based or password-based as described in RFC 4252. Key exchange is performed using diffie-hellman-group 14-sha1 The public key algorithm of the SSH transport implementation is ssh-rsa. For data encryption AES128-CTR, AES192-CTR and AES256-CTR are supported. For data integrity protection HMAC-SHA1,

	HMAC-SHA1-96 are supported.

7.5 Management Traffic Flow Control

The TOE uses ACL to deny unwanted network traffic on management interfaces and allow wanted 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, and TCP/UDP destination port, and then performs actions such as permit, or discard accordingly.

(FDP_IFC.1, FDP_IFF.1, FTA_TSE.1)

Table 7-6 SFR to TSF mapping

SFR	TSF
FDP_IFC.1	The TOE uses ACL to deny unwanted network traffic on management interfaces and allow wanted network traffic on management interfaces.
FDP_IFF.1	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, and TCP/UDP destination port, and then performs actions such as permit, or discard accordingly.
FTA_TSE.1	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, and TCP/UDP destination port, and then performs actions such as permit, or discard accordingly, thus being able to deny session establishment based on those criteria.

7.6 Security Management

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

- User management, including the user name and passwords.
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling of TLS for the communication between EMS and the TOE.

- Definition of IP addresses and address ranges for clients and server that are allowed to connect to the TOE.
- Set-up and modification of ACL policy.

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

Detailed functions mainly include:

- Support remote TOE management using TLS.
- 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 ACL filtering based on IP protocol number, source and/or destination IP address, or source and/or destination port.
- Support the address configuration of the RADIUS server.
- Support the address configuration of the Syslog server.
- Support the address configuration of the NTP server.
- Support the address configuration of the SFTP server.
- Support setting the time information on the TOE.

The TOE management can use two kinds of sessions for administrative activities based on different protocols:

- QX is a proprietary interface between EMS and TOE. EMS uses QX commands to implement OAM (Operation Administration and Maintenance) function on TOE. The TOE provides abundant QX commands to allow the users to manage the TOE.
- MML commands are used mainly for local maintenance tasks like fault location and software upgrades. For this evaluation, MML commands are used to up- and download files via the TOE's SFTP client.

Note that users cannot have QX and MML sessions at the same time.

(FMT_SMF.1, FMT_MSA.1/IFF, FMT_MSA.3/IFF)

Table 7-7 SFR to TSF mapping

SFR	TSF
FMT_SMF.1 FMT_MSA.1/IFF	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 mainly include: User management, including the user name and passwords. Access control management, including the association of users and corresponding privileged functionalities. Enabling/disabling of TLS for the communication between EMS and the TOE. Definition of IP addresses and address ranges for clients and server that are allowed to connect to the TOE. Set-up and modification of ACL policy. All of these management options are generally available via the EMS.

	Detailed functions mainly include: Support remote TOE management using TLS. Support SFTP 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 configuration of the RADIUS server. Support configuration of the Syslog server. Support configuration of the NTP server. Support configuration of the SFTP server. Support setting the time information on the TOE.
FMT_MSA.3/IFF	The ACL filtering mechanism is enforcing the Management Network Filtering SFP. By default, no ACL rules are configured therefore all traffic will be allowed to pass. Administrators and Super-Administrators can add, delete and modify ACL rules. The ACL rules will take effect immediately after they are added. The ACL filtering mechanism does only accept connections that are explicitly permitted in the ACL filtering rules. By adding corresponding ACL rules, Administrators and Super-Administrators can change the default behavior where all traffic is allowed to pass.

7.7 Time

The TOE provides its own clock and timestamps to correctly record logs in time sequence or other place wherever the time shall be used. The time information on the TOE can either be set by a user with sufficient access rights on the device or obtained from external NTP time sources.

(FPT_STM.1)

Table 7-8 SFR to TSF mapping

SFR	TSF
FPT_STM.1	The TOE provides its own clock and timestamps to correctly record logs in time sequence or other place wherever the time shall be used. The time information on the TOE can either be set by a user with sufficient access rights on the device or obtained from external NTP time sources.

7.8 Cryptographic functions

Cryptographic functions are required by security features as dependencies. The following cryptographic algorithms are supported:

1) The TOE supports symmetric encryption and decryption using the AES algorithm. The TOE support the following algorithms.

   GCM mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38D]**

   GCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38D]**

   CTR mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

   CTR mode, and cryptographic key sizes **192bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

   CTR mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

   CBC mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

   CBC mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

   AES-128/192/256 in CTR mode is used for encryption and decryption within SSH communication.

   AES-128/256 in GCM mode is used for encryption and decryption within TLS communication.

   AES-128/256 in CBC mode is used for encryption and decryption within TLS communication.

2) The TOE supports asymmetric authentication using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 with a key length of 2048 to 4096bits for SSH\TLS.
3) The TOE supports data integrity generation and verification using the HMAC-SHA1 (HMAC-SHA1-96) algorithm according to [RFC 2104], [FIPS 198-1] using key lengths of 160 (truncated to 96) bits. The data integrity protection mechanism is used as integrity protection for SSH communication.
4) The TOE supports keyed-hash message authentication using the HMAC-SHA256 and HMAC-SHA384 algorithm according to [FIPS 180-4]. This mechanism is used for the TLS communication. For all cipher suites defined in [RFC 5246] and [RFC 3268] it is used especially for data integrity protection. (For the remaining cipher suites defined in [RFC 5288] the mechanism is used according to [RFC 5288].)
5) SHA-256 and SHA-384 are used in TLS communication as hashing function.
6) The TOE supports hashing of data using PBKDF2 (HMAC-SHA256) algorithm according to [RFC2898] for password hashing. The iteration number is 10000. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE's deterministic random number generator. The TOE supports hashing of data using SHA1 according to [FIPS180-3] for SSH communication.
7) The TOE supports generation and distribution of cryptographic keys according to

diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048 bits according to [NIST SP 800-56A], [RFC 4253], [RFC 3526], [PKCS#3] for SSH/TLS.

8) The TOE supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT and adapting the method in [FIPS 186-4] Appendix B.3.3 and RSA key exchange according to [NIST SP 800-56B]. RSA keys generated have a key length of 2048 to 4096bits and are intended for usage with RSASSA-PKCS1-V1_5.
9) The TOE supports destruction of temporary session keys used for secure communication channels based on TLS or SFTP which are stored in volatile memory by erasing the corresponding area in memory reserved for the corresponding session. So the session keys are destroyed by the post-processing routines of the underlying trusted channel which are executed whenever a session is terminated for any reason.
10) The TOE supports the destruction of RSA private keys through full flash erase by overwriting with '1'. The destruction mechanism can only be executed after correct setting of a physical DIP switch that prevents accidental erase of the flash memory during normal operation.
11) The TOE supports the SSH protocol according to [RFC 4251], [RFC 4252], [RFC 4253], [RFC 4254] and the following cipher suites according to [RFC 4253]:
    - Diffie-hellman-group14-sha1 as key exchange algorithm of SSH.
    - AES-128-CTR/ AES-192-CTR/ AES-256-CTR encryption and decryption algorithm.
    - RSA (2048 to 4096 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (client) to the server.
    - HMAC-SHA1/ HMAC-SHA1-96 data integrity generation and verification algorithm.
12) The operations have been performed according to chap. 4.8 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bit entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The TOE ensures that TLS-based communication and SSH-based communication cannot be enabled before the DRNG is seeded.
    The DRNG complies with [NIST SP 800-90A] using HMAC-DRBG (SHA-256).

    (FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA1-96, FCS_COP.1/HMAC-SHA256, FCS_COP.1/HMAC-SHA384, FCS_CKM.1/DH, FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/PBKDF2, FCS_COP.1/SHA1, FCS_CKM.1/RSA, FCS_CKM.2, FCS_CKM.4/RSA, FCS_RNG.1)

Table 7-9 SFR to TSF mapping

SFR	TSF
FCS_COP.1/AES	The TOE supports symmetric encryption and decryption using the AES algorithm. The TOE supports the following algorithms. GCM mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38D]** GCM mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38D]** CTR mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]** CTR mode, and cryptographic key sizes **192bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]** CTR mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]**

	CBC mode, and cryptographic key sizes **256bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]** CBC mode, and cryptographic key sizes **128bits** that meet the following: [**FIPS 197], [NIST SP 800-38A]** AES-128/192/256 in CTR mode is used for encryption and decryption within SSH communication. AES-128/256 in GCM mode is used for encryption and decryption within TLS communication. AES-128/256 in CBC mode is used for encryption and decryption within TLS communication.
FCS_COP.1/RSA	The TOE supports asymmetric authentication using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 with a key length of 2048 to 4096bits for SSH\TLS.
FCS_COP.1/HMAC-SHA1 FCS_COP.1/HMAC-SHA1-96	The TOE supports data integrity generation and verification using the HMAC-SHA1 (HMAC-SHA1-96) algorithm according to [RFC 2104], [FIPS 198-1] using key lengths of 160 (truncated to 96) bits. The data integrity protection mechanism is used as integrity protection for SSH communication.
FCS_COP.1/HMAC-SHA256 FCS_COP.1/HMAC-SHA384	The TOE supports keyed-hash message authentication using the HMAC-SHA256 and HMAC-SHA384 algorithm according to [FIPS180-4]. This mechanism is used for the TLS communication. For all cipher suites defined in [RFC 5246] and [RFC 3268] it is used especially for data integrity protection. (For the remaining cipher suites defined in [RFC 5288] the mechanism is used according to [RFC 5288].)
FCS_CKM.1/DH	The TOE supports generation and distribution of cryptographic keys according to diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048 bits according to [NIST SP 800-56A], [RFC 4253], [RFC 3526], [PKCS#3] for SSH/TLS.
FCS_COP.1/SHA256	HMAC-DRBG using SHA-256 as its hash function
FCS_COP.1/SHA384	SHA256 and SHA384 are used in TLS communication as hashing function.
FCS_COP.1/PBKDF2	The TOE supports hashing of data using PBKDF2 (HMAC-SHA256) algorithm according to [RFC2898] for password hashing. The iteration number is 10000. The salt used in PBKDF2 is a 16 byte size random number obtained from the TOE’s deterministic random number generator.
FCS_COP.1/SHA1	The TOE supports hashing of data using SHA1 according to [FIPS180-3] for SSH communication.
FCS_CKM.1/RSA	The TOE supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT and adapting the method in [FIPS 186-4] Appendix B.3.3. RSA keys generated have a key length of 2048 to 4096bits and are intended for usage with RSASSA-PKCS1-V1_5.

FCS_CKM.2	The TOE supports generation and distribution of cryptographic keys according to diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048 bits according to [NIST SP 800-56A], [RFC 4253], [RFC 3526], [PKCS#3] for SSH/TLS and RSA key exchange according to [NIST SP 800-56B].
FCS_CKM.4/DH	The TOE supports destruction of temporary session keys used for secure communication channels based on TLS or SFTP which are stored in volatile memory by erasing the corresponding area in memory reserved for the corresponding session. So the session keys are destroyed by the post-processing routines of the underlying trusted channel which are executed whenever a session is terminated for any reason.
FCS_CKM.4/RSA	The TOE supports the destruction of RSA private keys through full flash erase by overwriting with '1'. The destruction mechanism can only be executed after correct setting of a physical DIP switch that prevents accidental erase of the flash memory during normal operation.
FCS_RNG.1	The operations have been performed according to chap. 4.8 of [AIS20]. For certified use of the TOE, the random seed of 32 bytes shall contain at least 128 bit entropy. The seed value is provided by the hardware TPM chip integrated in the SCC. The TOE ensures that TLS-based communication and SSH-based communication cannot be enabled before the DRNG is seeded. The DRNG complies with [NIST SP 800-90A] using HMAC-DRBG (SHA-256).

A Abbreviations, Terminology and References

A.1 Abbreviations

CC	Common Criteria
DCN	Data Communications Network (the management network)
EMS	Element Management System
LCT	Local Craft Terminal
LMT	Local Maintenance Terminal
MSTP	Multi-Service Transmission Platform
OSN	Optical Switch Node
OTN	Optical Transport Network
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RMT	Remote Maintenance Terminal
RSA	Rivest Shamir Adleman
SDH	Synchronous Digital Hierarchy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
WDM	Wavelength Division Multiplexing

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 in the content is the user of administrator group or super administrator group

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 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017
[AIS20]	Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Version 2.0, 2 December 1999
[FIPS 180-3]	FIPS PUB 180-3 – Secure Hash Standard (SHS), Octo, August 2015ber 2008
[FIPS 180-4]	FIPS PUB 180-4 – Secure Hash Standard (SHS)
[FIPS 186-4]	FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013
[FIPS 197]	FIPS PUB 197 – Advanced Encryption Standard (AES), November 26, 2001
[FIPS 198-1]	FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC), July 2008
[NIST SP 800-38A]	NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001
[NIST SP 800-38D]	NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007
[NIST SP 800-56A]	NIST Special Publication 800-56A – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013
[NIST SP 800-56B]	NIST Special Publication 800-56B Rev. 1 – Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, September 2014
[NIST SP 800-90A]	NIST Special Publication 800-90A Rev. 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
[PKCS#1 V2.1]	PKCS #1 v2.1: RSA Cryptography Standard, April 2004
[PKCS#3]	PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993

[RFC 2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC 2898] RFC 2898 - PKCS #5: Password-Based Cryptography Specification, version 2.0, September 2000

[RFC 3526] RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003

[RFC 4251] RFC 4251 – The Secure Shell (SSH) Protocol Architecture, January 2006

[RFC 4252] RFC 4252 - The Secure Shell (SSH) Authentication Protocol, January 2006

[RFC 4253] RFC 4253 - The Secure Shell (SSH) Transport Layer Protocol, January 2006

[RFC 4254] RFC 4254 - The Secure Shell (SSH) Connection Protocol, January 2006

[RFC 4346] RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[RFC 5246] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, August 2008