CC HUAWEI iMaster MAE V100R024C10 -Security Target V2.2

Issue V2.2

Date 2025-08-26

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: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page:

https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 About This Document

Change History

Version	Date	Change Description	Author
V1.0	2024-08-25	Initial Draft	Wangzunzhi, Rao Lei
V1.1	2024-10-24	Address Review Comment	Wangzunzhi
V1.2	2024-11-22	Address Review Comment	Wangzunzhi
V1.3	2025-02-22	Address Review Comment	Wangzunzhi
V1.4	2025-03-20	Address Review Comment	Wangzunzhi
V1.5	2025-03-28	Address Review Comment	Wangzunzhi
V1.6	2025-04-07	Address Review Comment	Wangzunzhi
V1.7	2025-04-09	Address Review Comment	Wangzunzhi
V1.8	2025-06-16	Address Review Comment	Wangzunzhi
V1.9	2025-06-19	Address Review Comment	Wangzunzhi
V2.0	2025-06-24	Address Review Comment	Wangzunzhi
V2.1	2025-08-20	Address Review Comment	Wangzunzhi
V2.2	2025-08-26	Address Review Comment	Wangzunzhi

2 Introduction

This Security Target is for the evaluation of HUAWEI iMaster MAE V100R024C10.

2.1 ST Reference

Title: CC HUAWEI iMaster MAE V100R024C10 - Security Target

Version: V2.2

Author: Huawei Technologies Co., Ltd.

Publication date: 2025-08-26

2.2 TOE Reference

TOE name: HUAWEI iMaster MAE V100R024C10

TOE version: V100R024C10SPC210

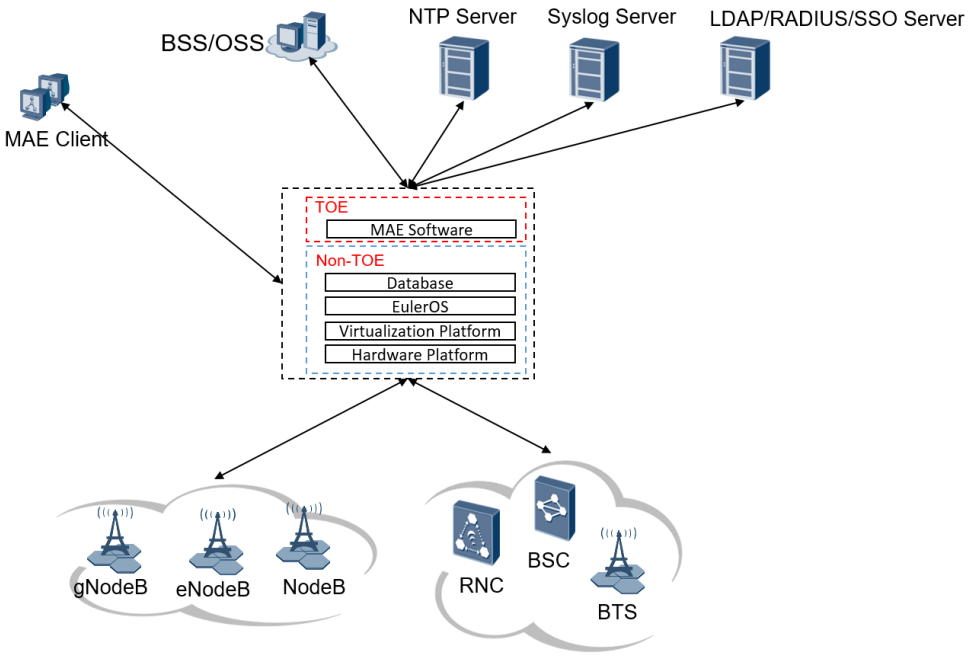
TOE Developer: Huawei Technologies Co., Ltd.

TOE release date: 2024-08-25

2.3 TOE Overview

MAE Network Management system provides centralized operation and maintenance (OM) for mobile network element management solution, provides external interfaces for interoperability with other systems. By providing automatic network OM capabilities, MAE can implement automatic network management.

Figure 2-1 MAE network positioning



The core and base of MAE is the CloudSOP platform. The CloudSOP platform provides the basic framework for OSS application deployment, monitoring and secondary development, as well as public services, such as user management, rights management, session management, log management, license management, alarm management, and topology management. The architecture of CloudSOP is highly reliable, flexible, open, and easy to be integrated, meeting the requirements from future OSS large-scale distributed clusters.

The TOE includes MAE software, which includes the CloudSOP platform, but does not include Database, Euler OS, Virtualization Platform, and Hardware Platform.

2.3.1 TOE Usage and Major Security Features

MAE is the software for managing mobile networks. It provides a centralized network management platform for supporting telecom operators in their long-term network evolution and shielding the differences between various network technologies. The MAE provides various OM solutions and meets various requirements, such as network deployment, network monitoring, network adjustment, and service management. The MAE focuses on continuous efforts that telecom operators have made for network OM and inherits the existing OM experience.

To cope with the TOE security threats, the TOE provides many security measures to effectively reduce security risks. The major security features implemented by the TOE and subject to evaluation are:

1. User management
2. Authentication
3. Access control
4. IP-based ACL
5. Communication security
6. User session management

7. Auditing
8. Security management function
9. Cryptographic functions

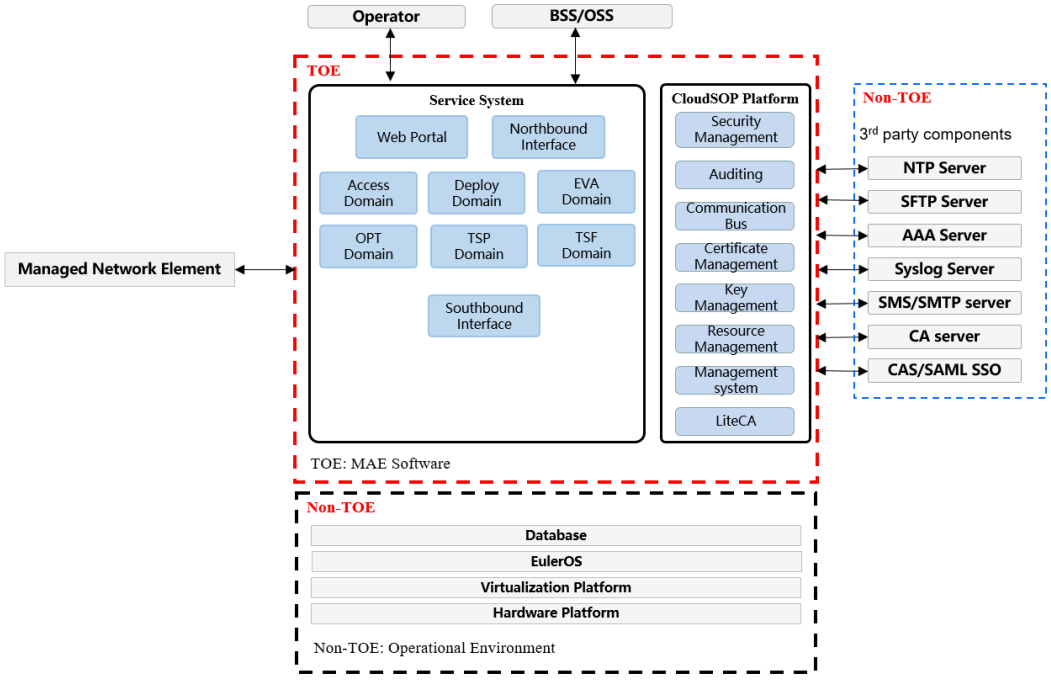
2.3.2 TOE Type

The TOE is a centralized network management software. The MAE is located at the management and control layer of the cloud network. It can manage and control ubiquitous network devices such as global system for mobile (GSM), wideband code division multiple access (WCDMA), long term evolution (LTE), 5G New Radio(5G NR). It provides open interfaces to quickly integrate with upper-layer application systems such as BSS and OSS. Various apps can be developed and customized to accelerate service innovation and achieve e-commerce-style operations.

The MAE software architecture is shown in the figure below. The CloudSOP platform is the underlying platform of the MAE software.

In the northbound direction, it provides Web Portals, Northbound interface for O&M personnel and BSS/OSS. In the southbound direction, it provides configuration and management capabilities for Huawei network devices and provides third-party driver management to manage and access third-party network adaptation drivers and third-party controllers outside the trusted zone. The system also interconnects with external SFTP servers, external AAA authentication servers, third-party Syslog servers, CA server and SMS/SMTP servers.

Figure 2-2 TOE overview



2.3.3 Non-TOE Hardware and Software

The MAE can be deployed in on-premises or private cloud mode. In this evaluation only on-premises deployment is in scope, and the following non-TOE Databases, Euler OS, Virtualization Platform, Hardware Platform, and Environment components are required.

The Non-TOE includes Databases, Euler OS, Virtualization Platform, Hardware Platform and Environment components.

Hardware Configurations:

Table 2-1 Hardware configurations requirements

Hardware	Model	Requirements
TaiShan 200 (Model 2280)	TaiShan 200 (Model 2280)	CPU: 2*920 48 Core/2.6GHz Memory: 24 * 32 GB Hard disk: 2/4 * 1.92 TB SSD

Configuration for the Databases, Euler OS, Virtualization Platform:

Table 2-2 Databases, Euler OS, Virtualization Platform version requirements

Item	Type	Version
Delivered software configurations	OS	EulerOS V200R011 and above
	Database	Gauss100 OLTP 1.7.1.SPC210 and above
Compatible software configurations	Virtualization software	FushionSphere OpenStack NFV_FusionSphere 22.1 and above

Configuration for the MAE Client:

Table 2-3 Client configuration requirements

Type	Requirements
CPU	The CPU clock speed is 2.6 GHz or higher, and the CPU has at least two physical cores.
Memory	4 GB or larger
Hard disk	500 GB or larger
Accessories	Integrated NIC, Gigabit Ethernet NIC, integrated audio card, internal speaker
OS	The following OSs are supported: Windows 10 (64-bit) Windows Server 2012 (64-bit) Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)
Web	You are advised to use Chrome or Firefox of the latest version. Chrome

Type	Requirements
browser	108.0 or later (stable channel version) and Firefox 102.8.0 or later (ESR version) are supported. Browsers of the latest versions usually contain more security updates and new features, which helps MAE provide more stable user experience. If you use a browser whose version is earlier than the recommended version, the product security may be affected, and certain functions may be abnormal.
Resolution	Optimal resolution: 1920 x 1080 Minimum resolution: 1366 x 768

Environment components:

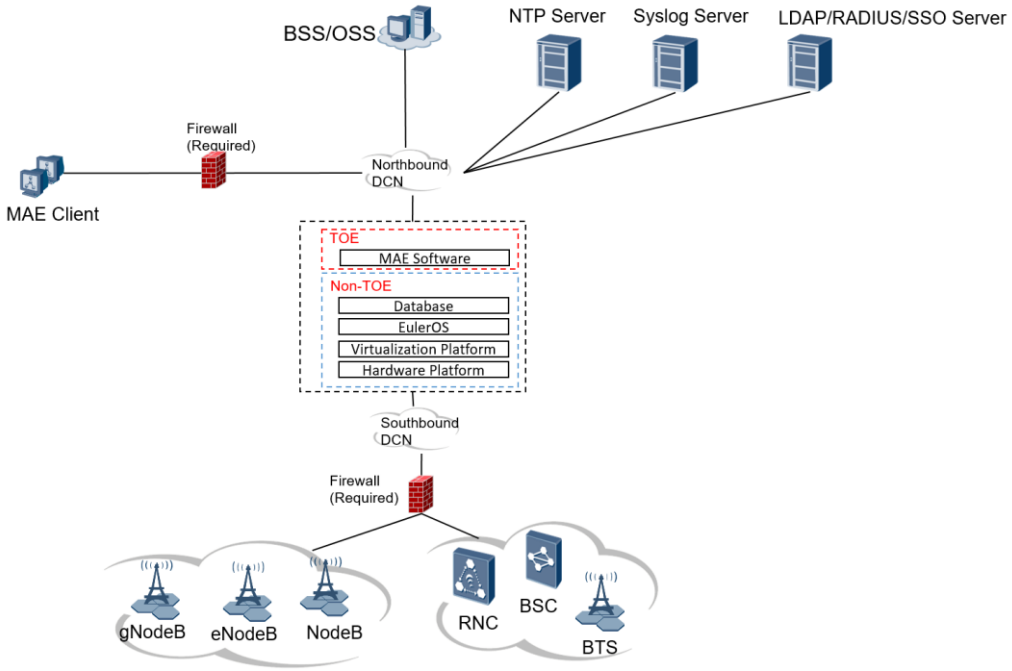
The environment for TOE also comprises the following components:

Table 2-4 Environment components

Component	Required/ Optional	Usage/Purpose Description for TOE Performance
Firewall	Required	Firewall used by customers to ensure communication security between different communication planes.
Network Elements (NEs)	Required	NEs that are managed by the TOE and support different communication protocols with the TOE.
Web portal, OSSs, service orchestrators and service applications	Required	The web portal connects to the TOE using HTTPS. And the OSSs, service orchestrators and service applications that connect to the TOE through external interfaces including SNMPv3, CORBA, SFTP, and some customized RESTful interfaces.
AAA server	Optional	The external AAA server used to authenticate users. The TOE can correctly leverage the services provided by this AAA server to authenticate administrators. The security mechanisms for remote LDAP/RADIUS authentication depend on the third-party AAA server. Security mechanisms, such as anti-brute force cracking, password complexity check, and anti-DoS attack, must be enabled on the third-party server. Especially the communication channel between TOE and RADIUS server should be protected.
Syslog server	Optional	Syslog server used to transmit syslog messages.
SFTP server	Optional	SFTP server used to upload performance files and back up NE data.

Component	Required/ Optional	Usage/Purpose Description for TOE Performance
SMS/SMTP server	Optional	MAE sends notifications by emails or messages.
CA server	Optional	CA server can apply for a certificate, update the certificate, and publish the CRL certificate revocation list (CRL) file.
NTP server	Required	NTP server is used to sync the time of the MAE server.

Figure 2-3 TOE physical environment



2.4 TOE Description

2.4.1 TOE Definition Scope

2.4.1.1 Physical Scope

The TOE is MAE software installed on-premises only.

Users can log in to the HUAWEI support website to download the software packages in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on the HUAWEI support website).

MAE software packages consist of binary compressed files. The following software packages and documents are required and are part of the TOE.

Table 2-5 TOE software list

Type	Delivery Item	Version
Software	MAE_V100R024C10SPC210_Access_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Deployment_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Jre_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Common_EulerOS-aarch64.zip MAE_V100R024C10SPC210_KPI_EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSP_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Evaluation_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Common_HD_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Optimization_EulerOS-aarch64.zip iPowerStar_3.1.5.1_MAE12410-EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSF_EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSF_CBB_EulerOS-aarch64.zip 5GtoBSuite_3.1.5.1_MAE12410-EulerOS-aarch64.zip MAE-OSMU_V100R024C10SPC210_EulerOS-aarch64_pkg.tar MAE-OSMU_V100R024C10SPC210_VNFLCM-IAASDeploy_EulerOS_pkg.tar	V100R024C10SPC210
Software Signature File	MAE_V100R024C10SPC210_Access_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Deployment_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Jre_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Common_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_KPI_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_TSP_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Evaluation_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Common_HD_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Optimization_EulerOS-aarch64.zip.p7s iPowerStar_3.1.5.1_MAE12410-EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_TSF_EulerOS-aarch64.zip.p7s	V100R024C10SPC210

Type	Delivery Item	Version
	MAE_V100R024C10SPC210_TSF_CBB_EulerOS-aarch64.zip.p7s 5GtoBSuite_3.1.5.1_MAE12410-EulerOS-aarch64.zip.p7s MAE-OSMU_V100R024C10SPC210_EulerOS-aarch64_pkg.tar.p7s MAE-OSMU_V100R024C10SPC210_VNFLCM-IAASDeploy_EulerOS_pkg.tar.p7s	
Platform Software	MAE_V100R024C10SPC210_CloudSOP_EulerOS-aarch64.zip	V100R024C10SPC210
Platform Software Signature File	MAE_V100R024C10SPC210_CloudSOP_EulerOS-aarch64.zip.p7s	V100R024C10SPC210

Table 2-6 TOE guidance list

Delivery Item	Document Obtaining Method	Version
(For Customer)iMaster MAE Product Documentation (EulerOS, TaiShan)-(V100R024C10_07)(HDX)-EN.hdx	The documents can be obtained from Huawei support.	Product version: V100R024C10, Library Version: 07, date: 2025-07-11
iPowerStar 3.1.5 Product Documentation 05-EN.hdx	The documents can be obtained from Huawei support.	Product version: V100R024C10(iPowerStar 3.1.5), Library Version: 05, date: 2025-03-28
5GtoB Suite 3.1.4 Product Documentation 02-EN.hdx	The documents can be obtained from Huawei support.	Product version: V100R024C10(5GtoB Suite 3.1.4), Library Version: 02, date: 2024-06-29
OSMU User Guide(EulerOS, TaiShan)(V100R024C10_06)(WORD)-EN.zip	The documents can be obtained from Huawei support.	Product version: V100R024C10, Issue: 06, date: 2024-08-20
iMaster MAE V100R024C10SPC210 Release Documents(EulerOS, TaiShan)-EN.zip	The documents can be obtained from Huawei support.	Product version: V100R024C10SPC210, date: 2025-01-22
CC HUAWEI iMaster MAE V100R024C10 - Operational user Guidance.pdf	The guidance for CC certification, delivered upon customer request by e-mail	Product version: V100R024C10, Issue: 02, date: 2025-03-13

Delivery Item	Document Obtaining Method	Version
CC HUAWEI iMaster MAE V100R024C10 - Preparative Procedures.pdf	The guidance for CC certification, delivered upon customer request by e-mail	Product version: V100R024C10, Issue: 02, date: 2025-06-25

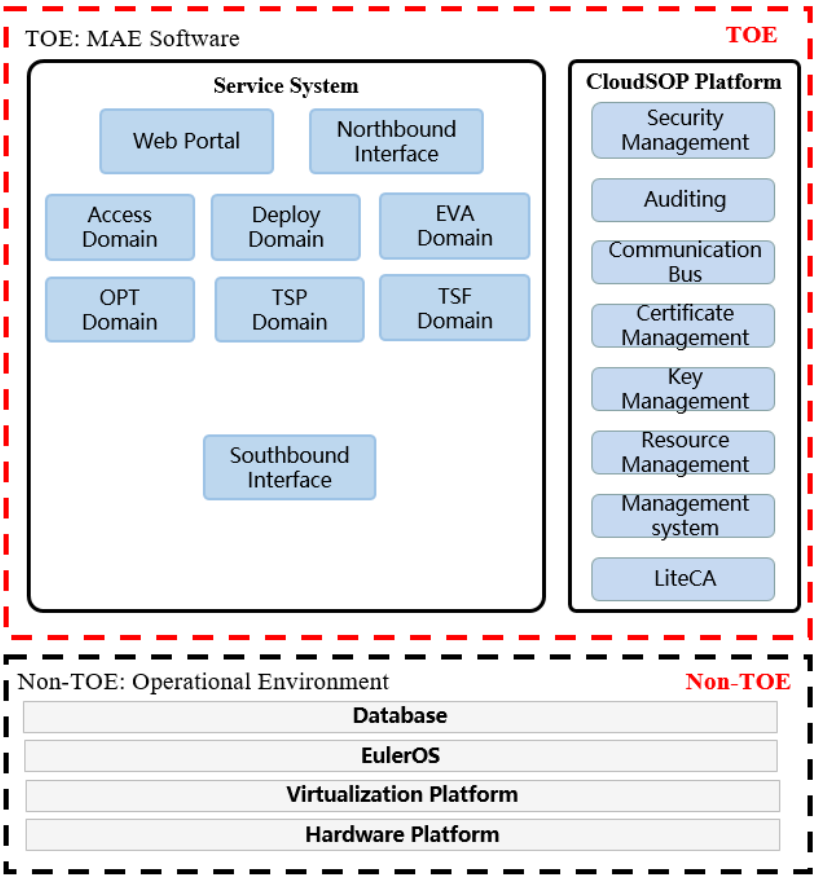
Users can log in to the Huawei support website to read the document directly or download the product documentation in accordance with the version of the TOE. The download file formats are *.hdx, *.chm or *.zip, user can download the *.hdx reader from the same website.

2.4.1.2 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 is a software running on the Euler OS.

The non-TOE part is marked with a black dashed line(include Database, Euler OS, Virtualization Platform, Hardware Platform).

Figure 2-4 TOE logical scope



The major security features of MAE that are subject to evaluation are:

User Management

On the management plane and O&M plane, the TOE provides user management based on role management.

It has the default user groups on the O&M plane including **Administrators, SMManagers, Maintenance Group, Operator Group, Operators, Guests, WebNIC User Group, AppUsers, Assurance User Group, CA Administrator Group, CA Operator Group, HOFS Group, Monitoring Group, NBI Admin Group, NBI OpenAPI User Group, NBI User Group and Viewers.**

It has the default user groups on the management plane including **Administrators, SMManagers, Operators, Monitors.**

The TOE also allows admin and the **SMManagers** to create custom user-defined User Group on all planes.

Authentication

The TOE authenticates all users who access the TOE by username and password. The TOE provides a local authentication mode. The TOE optionally provides authentication decisions obtained from an external AAA in the IT environment.

Access Control

The TOE supports SMManagers to grant permissions to users by means of security management. Then users can access and perform operations on the TOE and NEs based on their permissions.

IP-based ACL

The TOE offers a feature access control list (ACL) based on IP addresses for controlling which terminals can access the TOE through the TOE client.

Communication Security

The TOE supports encrypted transmission within the MAE server, between NEs and the MAE server, between a browser and the MAE server, and between an OSS/service application and the MAE server.

User Session Management

The TOE monitors and presents all online user sessions in real time. The TOE also provides session establishment, TSF-initiated session termination, user-initiated session termination.

Auditing

The TOE generates audit records for security-relevant management and stores the records in the database.

Logs record routine maintenance events of the TOE. For security purposes, 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 IP addresses and addition of services.

The TOE provides a Syslog solution to resolve the problem of limited storage space. Both security logs and operation logs can be saved on an external Syslog server.

The TOE also collects operation and security audit logs from managed network elements, and stores the logs in the database.

The query and filter functions are provided on the GUI, which allow authorized users to inspect audit logs.

Security Management Functions

The TOE offers security management for all management aspects of the TOE. Security management includes not only authentication and access control management, but also management of security-related data consisting of configuration profiles and runtime parameters. Security management can be customized.

Cryptographic Function

Cryptographic functions are dependencies required by security features. The TOE supports cryptographic algorithms as described in section 6.2.7 Cryptographic Support (FCS)

3 CC Conformance Claims

This ST is CC Part 2/3/4/5 conformant [CC]. The CC version of [CC] is CC:2022 Release 1.

This ST is EAL4 augmented with ALC_FLR.2.

The methodology to be used for evaluation is CEM:2022.

No conformance to a Protection Profile is claimed.

4 Security Problem Definition

4.1 Assumptions

A.PhysicalProtection The hardware that the TOE is running on is operated in a physically secure and well managed environment.

This document assumes that the software platform of the server that the TOE is running on (as listed in section 2.4.1 TOE Definition ScopeTOE Definition Scope) is protected against unauthorized physical access.

This document assumes that the database is protected against data file damage.

A.NetworkSegregation This document assumes that the network interface of the server and the TOE client will be accessed only through subnets where the TOE hosts are installed. The subnet is separate from public networks. Communications with the TOE server are performed through a firewall.

A.AdministratorBehaviour This document assumes that the super user **admin**, a user that belongs to the **SMManagers** and **Administrators** groups and the users of the underlying operating system will behave correctly and will not perform any harmful operation on the TOE.

A.NTP This document assumes that operating environment should provide an accurate time source, in order to ensure normal operations of the TOE server.

A.NetworkElements This document assumes that the managed network elements are trusted and can support the TLS /SNMPv3 /SSHv2 /SFTP connection with the TOE, and the private interface defined by Huawei.

A.Components It is assumed that the 3rd party components (like NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, and CA server) are considered trusted and will not attack the TOE.

A.TrustedPlatform This document assumes that the platform like OS, DB, hardware, virtual machine used by the TOE is trusted, and is properly hardened by the Administrator.

4.2 Threats

The threats described in this chapter are addressed by the TOE.

4.2.1 Assets and Agents

Asset	Description
TOE security function (TSF) data	The integrity and confidentiality of TSF data (such as user account information, passwords and audit records) should be protected against threat agents.
OM data	The confidentiality and integrity of the OM data of NEs (such as configuration data) should be protected against threat agents.

Agent	Description
Attacker	An external attacker, who is not a user of the TOE.
Eavesdropper	An eavesdropper, who has access to communication channels through which the OM and TSF data are transferred.
Unauthorized user	An unauthorized user of the TOE, who gains unauthorized access to the TOE.

4.2.2 Threats Addressed by the TOE

4.2.2.1 T.UnauthenticatedAccess

Threat: T.UnauthenticatedAccess	
Attack	An attacker who is not a user of the TOE, gains access to the TOE, modifies and compromises the confidentiality of the TSF and OM data.
Asset	TSF and OM data
Agent	An attacker

4.2.2.2 T.UnauthorizedAccess

Threat: T.UnauthorizedAccess	
Attack	An unauthorized user who gains unauthorized access to the TOE and compromises the confidentiality and integrity of the TSF and OM data. The user also performs unauthorized operations on NEs through the TOE.
Asset	TSF and OM data

Threat: T.UnauthorizedAccess	
Agent	An unauthorized user

4.2.2.3 T.Eavesdrop

Threat: T.Eavesdrop	
Attack	An eavesdropper (remote attacker) in the management network served by the TOE, who is able to intercept, modify, or re-use information assets that are exchanged between the TOE and NEs, between the TOE client and server, and between the TOE server and OSS/service orchestrator/service application client/CA server.
Asset	TSF and OM data
Agent	An eavesdropper

5 Security Objectives

5.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

1. **O.Communication** The TOE implements logical protection measures for network communication between the TOE and NEs from the operational environment, also for the network communication between the TOE and the OSS/service orchestrator/service application/CA server.
2. **O.Authorization** The TOE authorizes different roles that can be assigned to administrators in order to restrict the functions available to individual administrators, including limitation to session establishment and to actions performed on NEs.

   (The TOE authorizes different roles that can be assigned to users in order to restrict the functions available to a specific user.)
3. **O.Authentication** The TOE authenticates users before access to data and security functions is granted. The TOE provides configurable system policies to restrict user session establishment.
4. **O.Audit** The TOE generates, stores and reviews audit records for security-relevant administrator actions.
5. **O.SecurityManagement** The TOE manages security functions that it provides.

5.2 Security Objectives for the Operational Environment

1. **OE.NetworkElements** The operational environment ensures that the trusted NEs support the TLS /SNMPv3/SSHv2/SFTP/HTTPS connection with the TOE and private interface defined by Huawei.
2. **OE.Physical** The TOE is protected against unauthorized physical access.
3. **OE.NetworkSegregation** The operational environment protects the network where the TOE hosts are installed by separating it from the application (or public) network. A

firewall is installed between the TOE server and untrusted domain to filter unused communication ports.

4. **OE.Database** The operational environment protects the database against unauthorized physical access and data file damage.
5. **OE.AdministratorBehaviour** The super user **admin**, the users who belong to the **SMManagers** and **Administrators** groups and the users of the underlying operating system will behave correctly and will not perform any harmful operation on the TOE.
6. **OE.NTP** The operational environment provides an accurate time source, in order to ensure normal operations on the TOE server.
7. **OE.TrustedPlatform** The operation environment provides a trusted platform like OS, DB, hardware, virtual machine.
8. **OE.Components** The 3rd party components are considered trusted and will not attack the TOE. The administrator shall ensure the NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, and CA server is secured when these servers are used.

5.3 Security Objectives Rationale

5.3.1 Coverage

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

Security Objective for the TOE	Threat
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess and T.UnauthorizedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	T.UnauthorizedAccess and T.UnauthenticatedAccess
O.SecurityManagement	T.UnauthenticatedAccess, T.UnauthorizedAccess and T.Eavesdrop

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

Security Objective for the Operational Environment	Threat / Assumption
OE.NetworkElements	T.Eavesdrop A.NetworkElements
OE.Physical	A.PhysicalProtection T.UnauthenticatedAccess

Security Objective for the Operational Environment	Threat / Assumption
OE.NetworkSegregation	A.NetworkSegregation
OE.Database	A.PhysicalProtection T.UnauthenticatedAccess T.UnauthorizedAccess
OE. AdministratorBehaviour	A.AdministratorBehaviour
OE.NTP	A.NTP
OE.TrustedPlatform	A.TrustedPlatform
OE.Componets	A.Components

5.3.2 Sufficiency

The following rationale justifies that security objectives can counter each individual threat and that the achievement of each security objective can contribute to the removal, diminishing or mitigation of a specific threat:

Threat	Rationale for Security Objectives
T.UnauthenticatedAccess	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 permissions (O.SecurityManagement). The audit records record modification of usernames and passwords, user logins and logouts, login successes and failures (O. Audit). And the threat is countered by requiring the system and database to implement an authentication mechanism for its users (OE.Physical and OE.Database).
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism checking the operations that may be performed on the TOE and NEs (O.Authorization). The threat is also countered by authenticating the users in the TOE (O.Authentication). Access control mechanisms (including user levels and command levels) can be configured by users with sufficient permissions (O.SecurityManagement). The threat is also countered by audit records showing that if someone indeed performs unauthorized operations, they can be traced to (O.Audit). In addition, OE.Database ensures that user account data stored in the database will not be altered maliciously.
T.Eavesdrop	The threat of eavesdropping is countered by requiring

Threat	Rationale for Security Objectives
	security communications: - Securing network communication between the portal and MAE server over SFTP/HTTPS (O.Communication). - Over TLS/SSHv2/SFTP between the MAE server and NEs (O.Communication and OE.NetworkElements). - Over TLS/SNMPv3/SSHv2/SFTP/HTTPS between the MAE server and the OSS/service orchestrator/service application client (O.Communication). -Over CMPv2 between the MAE server and the CA server (O.Communication). Management of secure communication channels can be performed by users with sufficient permissions (O.SecurityManagement).

The following rationale justifies that security objectives for the operational environment can cover each individual assumption and that the achievement of each security objective can contribute to the consistency between a specific assumption and environment. If all security objectives for the operational environment are achieved, the intended usage is realized:

Assumption	Rationale for Security Objectives
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access is addressed by OE.Physical and OE.Database.
A.NetworkSegregation	The assumption that the TOE is not accessible through the application networks hosted by the networking device is addressed by OE.NetworkSegregation.
A.AdministratorBehaviour	The assumption that super user **admin** and the users who belong to the **SMManagers** and **Administrators** groups and the users of the underlying operating system will behave correctly and will not perform any harmful operation is addressed by OE.AdministratorBehaviour.
A.NTP	The assumption that the operational environment provides an accurate time source is addressed by OE.NTP
A.NetworkElements	The assumption that the managed network elements are trusted and support secure channel is addressed by OE.NetworkElements.
A.Components	The assumption that the 3rd party components are trusted and support secure channel is addressed by OE.Components.
A.TrustedPlatform	The assumption that the platform used by the TOE is trusted, and is properly hardened by **Administrators** is addressed by OE. TrustedPlatform.

The following table provides a matrix of TOE objectives and threats.

	T.Eavesdrop	**T.UnauthenticatedAccess**	**T.UnauthorizedAccess**
O.Communication	X		
O.Authentication		X	X
O.Authorization			X
O.Audit		X	X
O.SecurityManagement	X	X	X

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.
- ***Italicized and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

6.2 Security 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 audit data 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:**

1. **User login and logout**
2. **User account management**
   a. **Creating, deleting, and modifying user accounts**
   b. **Changing user passwords, mobile numbers and email addresses**
   c. **Granting access rights to user accounts**
3. **User group (role) management**
   a. **Creating, deleting, and modifying user groups**
   b. **Granting access rights to user groups**
4. **Security policy management**
   a. **Modifying password policies**
   b. **Modifying user account policies**
5. **User session management**
   a. **Kicking out individual user sessions**
6. **ACL management**
   a. **Creating, deleting, and modifying ACLs**
   b. **Specifying ACLs for individual user account.**
7. **Region, operation set and device set management**
8. **Audit log management**
9. **Certificate management**
10. **NE management**].

FAU_GEN.1.2

The TSF shall record within the audit data at least the following information:

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

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [**none**].

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 caused the event.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1

The TSF shall provide [**users attached to SMManagers, users with log query rights**] with the capability to read [**correspondent information**] from the audit data.

FAU_SAR.1.2

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

Application Note:

Operation rights required for querying and exporting logs vary based on log types.

Log Type	Permission
Security logs generated by all users	Query Security Log
System logs	Query System Log
Operation logs generated by all users	Query Operation Log
Operation logs generated by the current user	Query Personal Operation Log
Security logs generated by the current user	Query Personal Security Log

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 data, except the users who have been granted explicit read access.

6.2.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1

The TSF shall provide the ability to apply [**selection**] of audit data based on [**filter criteria of audit fields including start time, end time, operation, level, operator, terminal IP address, result, operation object and details**].

6.2.1.6 FAU_STG.2 Protected audit data storage

FAU_STG.2.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2

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

6.2.1.7 FAU_STG.4 Action in Case of Possible Audit Data Loss

FAU_STG.4.1

The TSF shall [**store audit records in the database and export them into files**] if the audit data storage exceeds [**occupies over the default value of 80% of the database capacity and lasts for over the default duration of 45 days**].

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.2 Completing Access Control

FDP_ACC.2.1

The TSF shall enforce the **[MAE access control policy]** on **[subjects: users, roles; objects: NE, NE attributes and System data; operation: access, query, create, modify, delete, start, and stop operations on the object]** and all operations among subjects and objects covered by SFP.

FDP_ACC.2.2

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

6.2.2.2 FDP_ACF.1 Security Attribute-Based Access Control

FDP_ACF.1.1

The TSF shall enforce the [**MAE access control policy**] to objects based on the following: [

1. **Subjects Users and their following security attributes:**
   a. **User ID**
   b. **User type**
   c. **User role assignment**
2. **Roles and their following security attributes:**
   a. **Role name**
3. **Objects:**
   NE and their security attributes:
   a. **Device ID**
   MML command groups and their security attributes:
   a. **Command group name**
   ]

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 operation.**
2. **Authorized roles are permitted access to operation.**

3. **Users can be configured with different user role to control the MAE access permission.**
4. **An operation set contains many operation rights that are assigned to specific user roles.**]

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**explicitly assigned security functions**].

Application Note: in TOE, there is operation set which are assigned to specific user to authorize access of subjects to objects.

FDP_ACF.1.4

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

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1

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

6.2.3.2 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.

6.2.3.3 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1

The TSF shall provide [**local, remote LDAP, remote RADIUS, CAS and SAML SSO capability**] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [

1. **When local authentication is enabled, user authentication is implemented by TOE itself.**
2. **When LDAP authentication is enabled, user authentication is implemented by a remote LDAP server.**
3. **When RADIUS authentication is enabled, user authentication is implemented by a remote RADIUS server.**

4. **When CAS and SAML SSO configuration is enabled, user authentication is implemented by the SSO server of the TOE, and the user can log into all trusted SSO clients of other TOE instances without being authenticated again after logging in to one of the trusted TOEs.**]

6.2.3.4 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions [**changing the password or user inactivity by default 30 minutes**].

6.2.3.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1

The TSF shall provide only [**an obscured feedback**] to the user while the authentication is in progress.

6.2.3.6 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. **Username**
3. **Password**
4. **User type**
5. **Mobile number, optional**
6. **Email address, optional**
7. **Welcome message, optional**
8. **Status of the account(locked/unlocked)**
9. **Login time policy**
10. **Client IP address policy**
11. **User role assignment**
12. **Maximum online sessions, optional**
13. **Account validity period (days), optional**
14. **The number of allowed login times, optional**
15. **Select the policy (Disable user, Delete user, Unlimited) if no login within a period (configurable days), optional**
16. **Auto-logout if no activity within configurable period, optional**
17. **Compulsory password renewal (Password validity period (days), In advance warning before password expires (days), Minimum password usage period (days)), optional**].

6.2.3.7 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1

The TSF shall detect when [***an administrator configurable positive integer within [1, 99]***] unsuccessful authentication attempts occur related to [**consecutive failed logins]**.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**lock the common user account or IP address for 30 minutes by default**].

6.2.3.8 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet: **[**

1. **Min. password length**
2. **Min. system administrator password length**
3. **Max. password length**
4. **Configurable number of latest passwords that cannot be reused**
5. **Password repetition not allowed within configurable number of months**
6. **Min. password usage period (days)**
7. **Password validity period (days)**
8. **Min. characters different between new and old passwords**
9. **Min. number of letters**
10. **Min. number of uppercase letters**
11. **Min. number of lowercase letters**
12. **Min. number of digits**
13. **Min. number of special characters**
14. **Password that cannot contain spaces**
15. **Password that cannot contain its username in reverse order**
16. **Password that cannot be an increasing, decreasing, or interval sequence of digits or letters**
17. **Policy about max. consecutive characters used in both username and password**
18. **Policy that the password cannot contain repeated character sequences**
19. **Max. times a character can consecutively occur**
20. **Password that cannot contain user's mobile number or email address**
21. **Password that cannot contain words in the uploaded password dictionary file or hacker language dictionary configured in the backend file]**

6.2.4 Security Management (FMT)

6.2.4.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

1. **Authentication mode configuration**
2. **User management**
3. **Role management**
4. **Account policy**
5. **Password policy**
6. **Audit log management**
7. **Certificate management**
8. **NE management**
9. **Client IP Address Policies (ACL)**
10. **Login time policy**
11. **Configuration of the time interval of user inactivity for terminating an interactive session**
12. **Command group management**
13. **Configuration of trusted channels for connecting to the external entities**
14. **Certificate Authority Service management**

].

6.2.4.2 FMT_SMR.1 Security Roles

FMT_SMR.1.1

The TSF shall maintain the roles: [

1. **Administrators**
2. **SMManagers**
3. **Operator Group**
4. **CA Administrator Group**
5. **CA Operator Group**
6. **user-defined User Group**].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.4.3 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [***determine the behaviour of, disable, enable***] the functions [**all the security functions defined in FMT_SMF.1**] to [**users assigned with roles as defined in FMT_SMR.1 or with explicitly assigned security functions**].

Application Note:

The detail privilege of each role is defined in the following table:

Role Name	Security Functions
Administrators	Certificate management Command group management NE management
SMManagers	Authentication mode configuration User management Role management Account policy Password policy Audit log management Client IP Address Policies (ACL) Login time policy Configuration of the time interval of user inactivity for terminating an interactive session
Operator Group	NE Management Command group management Configuration of trusted channels for connecting to the external entities
CA Administrator Group	Certificate Authority Service management
CA Operator Group	Certificate Authority Service management
user-defined User Group	Granted by SMManagers

6.2.4.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1

The TSF shall restrict the ability to [***query, modify, delete***] the [**certificates, private keys, and symmetric keys**] to [**Users assigned with roles as defined in FMT_SMR.1 or with explicitly assigned security functions**].

6.2.4.5 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1

The TSF shall enforce the [**MAE access control policy**] to restrict the ability to [***query, modify***] the security attributes [**all the security attributes defined in FDP_ACF.1 and FIA_ATD.1**] to [**Users assigned with roles as defined in FMT_SMR.1 or with explicitly assigned security functions**].

6.2.4.6 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1

The TSF shall enforce the [**MAE access control policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow [**Users assigned with roles as defined in FMT_SMR.1 or with explicitly assigned security functions**] to specify alternative initial values to override the default values when an object or information is created.

6.2.5 TOE Access (FTA)

6.2.5.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on [

a. User identity (username and password)

b. Client IP address policies (IP address range for login)

c. Login time policies (limited time segment for account login)

d. User lock status and enablement status

e. Password validity period (days)

f. Maximum online sessions

g. System login mode]

Application Note:

System login mode only affects local user login from web interfaces, and does not affect third-party user login.

6.2.5.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [**administrator-configured time interval, by default 30 minutes of user inactivity**].

6.2.5.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.5.4 FTA_TAH.1 TOE Access History

FTA_TAH.1.1

Upon successful session establishment, the TSF shall display the [***date, time, location***] of the last successful session establishment to the user.

FTA_TAH.1.2

Upon successful session establishment, the TSF shall display the [***date, time, location***] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3

The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

6.2.6 Trusted Path/Channels (FTP)

6.2.6.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [***remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure and modification]*.**

FTP_TRP.1.2

The TSF shall permit [***remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [***remote management***].

6.2.6.2 FTP_ITC.1 External System Inter-TSF Trusted Channel

FTP_ITC.1.1

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

FTP_ITC.1.2

The TSF shall permit [***the TSF and (the external system including the OSS, service orchestrator, service application and 3rd party component)]*** to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**authentication, dumping audit logs, backing up NE Data and restoring NE data**].

6.2.6.3 FTP_ITC.1 NE Inter-TSF Trusted Channel

FTP_ITC.1.1

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

FTP_ITC.1.2

The TSF shall permit [***the TSF and (the NEs)]*** to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**managing NE devices**].

6.2.7 Cryptographic Support (FCS)

6.2.7.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1/PBKDF2

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[PBKDF2]** and specified cryptographic key sizes **[256 bits]** that meet the following: **[RFC8018 chapter 5.2]**

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, 3072 bits, 4096 bits, 8192 bits]** that meet the following: **[FIPS 186-4 appendix B.3]**

FCS_CKM.1.1/ECDSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[ECDSA]** and specified cryptographic key sizes **[256 bits(secp256r1), 384 bits(secp384r1), 521 bit(secp521r1)]** that meet the following: **[FIPS 186-4 appendix B.4]**

6.2.7.2 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1

The TSF shall perform [**cryptographic key backup**] in accordance with a specified cryptographic key access method [**encrypted by the encryption key specified by the user**] that meets the following: [**none**].

6.2.7.3 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1/SYM

The TSF shall destroy **[encryption Key]** when **[*no longer needed*].**

FCS_CKM.6.1/SIG

The TSF shall destroy **[digital signature RSA&ECDSA private key]** when **[*no longer needed*].**

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **[overwriting with 0]** that meets the following: **[none].**

6.2.7.4 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/SYM

The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified cryptographic algorithm **[AES GCM Mode]** and cryptographic key sizes **[256 bits]** that meet the following: **[FIPS 197 chapter 5, NIST SP 800-38A chapter 6.2]**

FCS_COP.1.1/PBKDF2

The TSF shall perform **[password hashing]** in accordance with a specified cryptographic algorithm **[PBKDF2 (SHA256)]** and cryptographic key sizes **[None]** that meet the following: **[RFC8018 chapter 5.2].**

FCS_COP.1.1/RSASSA

The TSF shall perform **[digital signature operation]** in accordance with a specified cryptographic algorithm **[RSASSA-PSS, RSASSA-PKCS1-v1_5]** and cryptographic key sizes **[2048bits, 3072bits, 4096bits, 8192bits]** that meet the following: **[RFC8017 section 8.1 (RSASSA-PSS) and 8.2 RSASSA-PKCS-v1_5), FIPS 186-4 chapter 5].**

FCS_COP.1.1/ECDSA

The TSF shall perform **[digital signature operation]** in accordance with a specified cryptographic algorithm **[ECDSA]** and cryptographic key sizes **[256bits, 384bits, 521bits]** that meet the following: **[ANSI X9.62，FIPS 186-4 chapter 6].**

6.2.7.5 FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.1.1/JDK

The TSF shall perform deterministic random bit generation services using [**NativePRNGBlocking**] in accordance with [**NIST SP 800-90A Rev. 1, FIPS 140-2**] after initialization.

FCS_RBG.1.1/OPENSSL

The TSF shall perform deterministic random bit generation services using [**CSPRNG**] in accordance with [**NIST SP 800-90A Rev. 1**] after initialization.

FCS_RBG.1.2

The TSF shall use a [***/dev/random***] for initialization and reseeding.

FCS_RBG.1.3/JDK

The TSF shall update the DRBG state by [***reseeding***] using a [***/dev/random***] in the following situations: [***on the condition:[When the entropy value in the entropy pool is less than 1024 bits]***] in accordance with [**NIST SP 800-90A Rev. 1**].

FCS_RBG.1.3/OPENSSL

The TSF shall update the DRBG state by [***reseeding***] using a [***/dev/random***] in the following situations: [***on the condition:[OPENSSL will automatically reseed every 7 minutes or after obtaining 2^16 random numbers. The product will actively call OPENSSL's RAND_seed to reseed after obtaining 2^23-1 random numbers.]***] in accordance with [**NIST SP 800-90A Rev. 1**].

6.2.7.6 FCS_RBG.2 Random bit generation (external seeding)

FCS_RBG.2.1

The TSF shall be able to accept a minimum input of [**256 bits**] from a TSF interface for obtaining entropy.

6.2.8 Protection of The TSF (FPT)

6.2.8.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1

The TSF shall protect TSF data from **[*disclosure, modification*]** when it is transmitted between separate parts of the TOE.

6.2.8.2 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [**CMPv2**].

FPT_ITI.1.2

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [**rejection of the data**] if modifications are detected.

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.

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_SAR.3	O.Audit
FAU_STG.2	O.Audit
FAU_STG.4	O.Audit
FDP_ACC.2	O.Authorization
FDP_ACF.1	O.Authorization
FIA_UID.2	O.Audit O.Authentication O.Authorization
FIA_UAU.2	O.Authentication O.Authorization
FIA_UAU.5	O.Authentication O.Authorization
FIA_UAU.6	O.Authentication O.Authorization

Security Functional Requirements	Objectives
FIA_UAU.7	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization O.SecurityManagement
FIA_AFL.1	O.Authentication O.Authorization
FIA_SOS.1	O.Authentication O.SecurityManagement
FMT_SMF.1	O.Audit O.Authentication O.Authorization O.Communication O.SecurityManagement
FMT_SMR.1	O.Authorization
FMT_MOF.1	O.SecurityManagement
FMT_MTD.1	O.SecurityManagement
FMT_MSA.1	O.Authorization
FMT_MSA.3	O.Authorization
FTA_TSE.1	O.Authentication
FTA_SSL.3	O.Authentication
FTA_SSL.4	O.SecurityManagement
FTA_TAH.1	O.Authentication
FTP_TRP.1	O.Communication
FTP_ITC.1/External System	O.Communication
FTP_ITC.1/NE	O.Communication
FCS_CKM.1.1/PBKDF2	O.SecurityManagement
FCS_CKM.1.1/RSA	O.Communication
FCS_CKM.1.1/ECDSA	O.Communication
FCS_CKM.3	O.SecurityManagement
FCS_CKM.6.1/SYM	O.Communication O.SecurityManagement
FCS_CKM.6.1/SIG	O.Communication
FCS_CKM.6.2	O.Communication

Security Functional Requirements	Objectives
	O.SecurityManagement
FCS_COP.1.1/SYM	O.SecurityManagement
FCS_COP.1.1/PBKDF2	O.Authentication O.SecurityManagement
FCS_COP.1.1/RSASSA	O.Communication
FCS_COP.1.1/ECDSA	O.Communication
FCS_RBG.1	O.Communication O.SecurityManagement
FCS_RBG.2	O.Communication O.SecurityManagement
FPT_ITT.1	O.Communication
FPT_ITI.1	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.

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by (FAU_GEN.1). Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the identification mechanism (FIA_UID.2). Audit records are stored in the database, and are filtered to read and search with conditions, and restricted audit review requires authorized users (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3). Management functionality for the audit mechanism is spelled out in (FMT_SMF.1). The audit record is stored in the database, and exported into a file if the size of the audit record exceeds the configured maximum size (FAU_STG.2, FAU_STG.4).
O.Communication	Communication security is implemented by data integrity protection (FPT_ITI.1) between TOE and the CA server, trusted channels (FTP_ITC.1/External System, FTP_ITC.1/NE) between TOE and external servers, and (FTP_TRP.1) between TOE and the web clients. Performance and inventory text files are transmitted to the OSS/service application. (FTP_TRP.1) Management functionality to configure the trusted channel for NE communication is provided in (FMT_SMF.1). Services are accessed through the TLS security protocol.

Security objectives	Rationale
	(FPT_ITT.1) The TOE integrates a private CA called LiteCA for issuing TLS certificates to internal services or NEs (FCS_COP.1.1/RSASSA, FCS_COP.1.1/ECDSA). The certificate key type can be either RSA (FCS_CKM.1.1/RSA) or ECDSA (FCS_CKM.1.1/ECDSA), (FCS_RBG.1 and FCS_RBG.2 provides the random number required by FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECDSA). When the digital signature key is not required, the digital signature key is destroyed.(FCS_CKM.6.1/SIG, FCS_CKM.6.2)
O.Authentication	User authentication (including re-authentication) is implemented by (FIA_UAU.2, FIA_UAU.5, FIA_UAU.6) and supported by individual user identities in (FIA_UID.2). The necessary user attributes (passwords) are spelled out in (FIA_ATD.1). The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for login (FTA_TSE.1), and a password policy (FIA_SOS.1). Management functionality is provided in (FMT_SMF.1). The TOE logs off sessions when they are inactive for a configured period of time (by default 30 minutes) (FTA_SSL.3). The session establishment shall be denied based on security attributes (FTA_TSE.1). Authentication feedback information is protected by (FIA_UAU.7). TOE shall display access history of the last successful and unsuccessful logins (FTA_TAH.1). For password verification hash values of passwords are used which are generated using PBKDF2(FCS_COP.1.1/2). The authentication mechanism for NBIs and NEs to connect to MAE is also implemented by FIA_UAU.2.
O.Authorization	The requirement for access control is spelled out in (FDP_ACC.2), and the access control policies are modeled in (FDP_ACF.1) for accessing the MAE server. Unique user IDs are necessary for access control (FIA_UID.2), and user authentication (FIA_UAU.2, FIA_UAU.5). User-related attributes are spelled out in (FIA_ATD.1). Access control is based on the definition of roles as subjects and functions as objects (FMT_SMR.1). Management functionality for the definition of access control policies is provided (FMT_MSA.1, FMT_MSA.3, FMT_SMF.1). User re-authentication is implemented by (FIA_UAU.6). If a user fails to log in to the system for multiple consecutive times, the locking policy for the account and IP address is executed (FIA_AFL.1).
O.SecurityManagement	Management functionality is provided in (FMT_SMF.1/FIA_ATD.1/FIA_SOS.1/FMT_MOF.1/FTM_MTD.1/FTA_SSL.4). The symmetric encryption key is generate by use PBKDF2(FCS_CKM.1.1/PBKDF2), (FCS_RBG.1 and FCS_RBG.2 provides the random number required by

Security objectives	Rationale
	FCS_CKM.1.1/PBKDF2). The system backs up the symmetric encryption key.(FCS_CKM.3) When the symmetric encryption key is not required, the symmetric encryption key is destroyed.(FCS_CKM.6.1/SYM, FCS_CKM.6.2) The irreversible encryption algorithms PBKDF2 are used to protect web user passwords.(FCS_COP.1.1/PBKDF2) The AES algorithm is used to encrypt service data(such as configuration data). (FCS_COP.1.1/SYM)

The following table provides a matrix of SFRs and the security objectives.

	O.Audit	O.Authorization	O.Authentication	O.Communication	O.Security Management
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_STG.2	X				
FAU_STG.4	X				
FDP_ACC.2		X			
FDP_ACF.1		X			
FIA_UID.2	X	X	X		
FIA_UAU.2		X	X		
FIA_UAU.5		X	X		

	O.Audit	O.Authorization	O.Authentication	O.Communication	O.Security Management
FIA_UAU.6		X	X		
FIA_UAU.7			X		
FIA_ATD.1		X	X		X
FIA_AFL.1		X	X		
FIA_SOS.1			X		X
FMT_SMF.1	X	X	X	X	X
FMT_SMR.1		X			
FMT_MOF.1					X
FMT_MTD.1					X
FMT_MSA.1		X			
FMT_MSA.3		X			
FTA_TSE.1			X		
FTA_SSL.3			X		
FTA_SSL.4					X
FTA_TAH.1			X		
FTP_TRP.1 Trusted Path				X	
FTP_ITC.1/External System				X	
FTP_ITC.1/NE				X	

	O.Audit	O.Authorization	O.Authentication	O.Communication	O.Security Management
FCS_CKM.1.1/PBKDF2					X
FCS_CKM.1.1/RSA				X	
FCS_CKM.1.1/ECDSA				X	
FCS_CKM.3					X
FCS_CKM.6.1/SYM				X	X
FCS_CKM.6.1/SIG				X	
FCS_CKM.6.2				X	X
FCS_COP.1.1/SYM					X
FCS_COP.1.1/PBKDF2			X		X
FCS_COP.1.1/RSASSA				X	
FCS_COP.1.1/ECDSA				X	
FCS_RBG.1				X	X
FCS_RBG.2				X	X
FPT_ITT.1				X	
FPT_ITI.1				X	

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL4 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.

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Resolved by external time source. The audit time depends on the reliable time stamp. Reliable time stamp depends on external time sources
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.2 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3
FIA_UID.2	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.1
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.1	None	None
FMT_SMF.1	None	None

Security Functional Requirement	Dependencies	Resolution
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FTA_TSE.1	None	None
FTA_SSL.3	FMT_SMR.1	FMT_SMR.1
FTA_SSL.4	None	None
FTA_TAH.1	None	None
FTP_TRP.1	None	None
FTP_ITC.1/External System	None	None
FTP_ITC.1/NE	None	None
FCS_CKM.1.1/PBKDF2	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1.1/SYM FCS_RBG.1 FCS_CKM.6.1/SYM FCS_CKM.6.2
FCS_CKM.1.1/RSA	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1.1/RSASSA FCS_RBG.1 FCS_CKM.6.1/SIG FCS_CKM.6.2
FCS_CKM.1.1/ECDSA	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1.1/ECDSA FCS_RBG.1 FCS_CKM.6.1/SIG FCS_CKM.6.2
FCS_CKM.3	[FDP_ITC.1, or	FCS_CKM.1.1/PBKD

Security Functional Requirement	Dependencies	Resolution
	FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5]	F2 FCS_CKM.1.1/RSA FCS_CKM.1.1/ECDSA
FCS_CKM.6.1/SYM	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1.1/PBKDF2
FCS_CKM.6.1/SIG	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1.1/RSA FCS_CKM.1.1/ECDSA
FCS_CKM.6.2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1.1/PBKDF2 FCS_CKM.1.1/RSA FCS_CKM.1.1/ECDSA
FCS_COP.1.1/SYM	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1.1/PBKDF2 FCS_CKM.6.1/SYM FCS_CKM.6.2
FCS_COP.1.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.6	None Only irreversible hashing of password, and the dependency is not required.
FCS_COP.1.1/RSASSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1.1/RSA FCS_CKM.6.1/SIG FCS_CKM.6.2
FCS_COP.1.1/ECDSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1.1/ECDSA FCS_CKM.6.1/SIG FCS_CKM.6.2
FCS_RBG.1	[FCS_RBG.2, or FCS_RBG.3] FPT_FLS.1 FPT_TST.1	FCS_RBG.2 FPT_FLS.1 and FPT_TST.1 are not required. JDK SecureRandom does not require a self-test upon invocation, as it is

Security Functional Requirement	Dependencies	Resolution
		designed to be a cryptographically strong pseudo-random number generator (CSPRNG). It automatically ensures compliance with FIPS 140-2 randomness requirements and produces non-deterministic output. OpenSSL's cryptographically secure pseudo-random number generator (CSPRNG) ensures that it is properly seeded and maintained, which includes internal integrity checks.
FCS_RBG.2	FCS_RBG.1	FCS_RBG.1
FPT_ITT.1	None	None
FPT_ITI.1	None	None

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] Part 3. The following table provides an overview of the assurance components that form the assurance level for the TOE.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation

Assurance class	Assurance components
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.5 Security Assurance Requirements Rationale

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

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 User Management

The TOE supports user management. User management involves user permission management, region management, and user maintenance and monitoring. User management grants permissions to users with different responsibilities, and adjusts the permissions based on service changes. This ensures that users have the necessary permissions to perform tasks and that other management tasks are carried out in order, avoiding unauthorized and insecure operations.

Security administrators can create roles, assign operation rights to the roles, and attach users to roles to grant them corresponding operation rights based on service requirements. This implements quick user authorization, improving O&M efficiency.

To improve management efficiency, security administrators divide the network into regions based on service requirements and allow different personnel to manage users and services in different regions.

During user permission maintenance period, security administrators can view and modify user, role, and operation set information, and monitor user sessions and operations in real time, ensuring system security.

The default roles on the management plane are listed in the table below.

Role Name	Description
Administrators	The user group has all rights except user management, query security log, query personal security log and view online users.
SMManagers	The user group has permission to manage users, query security logs, view online users, and update ACL policies.
Operators	The user group has permission to perform non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, trace server product

Role Name	Description
	tool, configure NAT tool, information collection, trouble shooting, emergency system, cloud service management, infrastructure, commissioning wizard, etc.
Monitors	The user group has permission to monitor non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, trace server product tool, configure NAT tool, information collection, trouble shooting, emergency system, cloud service management, infrastructure, commissioning wizard, etc.

The default roles on the O&M plane are listed in the table below.

Role Name	Description
Administrators	The user group has all rights except user management, query security log and view online users.
SMManagers	The user group has permission to manage users, manage licenses, query security logs, view online users, and update ACL policies.
NBI User Group	The user group has the permissions on operations and interface configurations for all northbound interfaces.
Guests	The user group has the permissions only to view fault management and system operations and to query personal operation logs.
Maintenance Group	The user group has permissions to maintain the OSS and NEs. Users attached to this role can perform operations such as adding, deleting, modifying, and querying the OSS and NEs.
Operator Group	The user group has NE maintenance-related permissions, such as fault management, log management, topology management, and system operations. Users attached to this role can set network device parameters, monitor device status, handle faults, and upgrade software.
WebNIC User Group	The user group has WebNIC-related permissions, such as collecting network information, querying all operation logs, and managing tasks.
Operators	The user group has rights of maintenance management, configuration management, northbound management, and assist tool management.
AppUsers	The user group has rights of application access.
Assurance User Group	The user group has MAE-Optimization/MAE-Evaluation system services-related permissions, such as querying OSS basic information, managing threshold alarms, and issuing MML commands to NEs.

Role Name	Description
CA Administrator Group	The user group has the operation permissions on all functions of the CA service.
CA Operator Group	The user group has the operation permissions on some functions of the CA service.
HOFS Group	The user group has the File Management Operation Set permission.
Monitoring Group	The user group has permissions only to perform basic operations such as browsing and viewing.
NBI Admin Group	The user group has the permissions on operations and interface configurations for all management interfaces.
NBI OpenAPI User Group	The user group has device-level operation rights for all objects and application-level operation rights for northbound open APIs.
Viewers	The user group has rights of maintenance browsing, configuration browsing, and northbound data browsing.

The role **Administrators** is to administer the TOE; the role **SMManagers** is the security role of the TOE, who can complete security management of TSF data, user management, audit review and authorization.

The TOE also has a default and super user **admin**, who belongs to **Administrators** and **SMManagers**. The super user **admin** can complete all the functions, including security and administrative functions.

(FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1)

Note: The role is the same as user group in the TOE. The user roles can be managed at the ManagementWeb and the OMWeb interface.

7.1.2 Authentication

Authentication based on security attributes is enforced prior to any other interaction with the TOE for all interfaces of the TOE(FIA_UAU.2).

At the ManagementWeb and OMWeb interfaces, the TOE provides the following security mechanisms:

The TOE identifies administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces(FIA_UID.2).

The TOE authenticates users based on the user attributes defined in FIA_ATD.1. The passwords should meet the defined password policy; otherwise the input of password shall be refused. When a user uses an expired password for login, the system will refuse the login request, the user must request the administrator to reset the password (the administrator can deactivate the password expiration policy).

The TOE verifies that the ManagementWeb and OMWeb user passwords meets the following password policies: [

1. Min. password length
2. Max. system administrator password length
3. Max. password length
4. Configurable number of latest passwords that cannot be reused
5. Password repetition not allowed within the configurable number of months
6. Min. password usage period (days)
7. Password validity period (days)
8. Min. characters different between new & old passwords
9. Min. number of letters
10. Min. number of uppercase letters
11. Min. number of lowercase letters
12. Min. number of digits
13. Min. number of special characters
14. Password that cannot contain spaces
15. Password that cannot contain its username in reverse order
16. Password that cannot be an increasing, decreasing, or interval sequence of digits or letters
17. Policy about max. consecutive characters used in both the username and password
18. Policy that the password cannot contain repeated character sequences
19. Max. times a character can consecutively occur
20. Password that cannot contain user's mobile number or email address
21. Password that cannot contain words in the password dictionary or hacker language dictionary](FIA_SOS.1, FTA_TSE.1)

Advanced parameters have such as Min. Different characters between new and old passwords, Min. Letter, Min. Lowercase, Min. Numbers.

User IDs are unique within the TOE and are stored together with associated passwords and other attributes including extended security attributes in the TOE's configuration database. If the user is in the disabled status, the login will be refused.

At the ManagementWeb and OMWeb interface, if the user password is entered incorrectly for five consecutive times within 10 minutes, the client IP address will be locked for 10 minutes(FIA_AFL.1).

At the ManagementWeb and OMWeb interface, the TOE supports the account and IP address lockout policy on the **Account Policy** page. The default account lockout policy is that when you enter the password incorrectly for 5 consecutive times within 10 minutes, the account will be locked for 30 minutes and automatically unlocked afterwards. The default IP address lockout policy is that when you enter the password incorrectly for 10 consecutive times within 1 minute, the IP address will be locked for 30 minutes and automatically unlocked afterwards(FIA_AFL.1).

At the ManagementWeb and OMWeb interface, if three accounts using a client IP address are locked within 10 minutes, this client IP address will be locked for 30 minutes(FIA_AFL.1).

At the ManagementWeb and OMWeb interface, all users can log in to the O&M plane again after the lockout period expires. Local users can also contact security administrators to unlock their accounts for re-login(FIA_AFL.1).

The user authentication modes include local authentication and remote authentication. In remote authentication mode, users are authenticated by an AAA server through AAA protocols. The TOE supports Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS) for AAA authentication. The TOE supports CAS SSO. SSO configuration allows users to access multiple mutually trusted application systems after only one login authentication. (FIA_UAU.5).

The TOE can re-authenticate the user under the condition of changing passwords (FIA_UAU.6).

The TOE displays the asterisk (*) that has the same length as the entered password, and returns a username or password error when login failed (FIA_UAU.7).

For other interfaces, the TOE provides the following security mechanisms:

All interfaces provide certificate authentication or user name password authentication to ensure that all interfaces verify the legitimacy of the peer.(FIA_UAU.2)

7.1.3 Access Control

At the ManagementWeb and OMWeb interface, the TOE enforces an authorization policy by defining access rights that are assigned to users and roles by the security roles or the super user **admin**.

At the OMWeb interface, the TOE enforces the access control policy on users and groups as subjects, domains as objects, functional operations issued by subjects on objects. The domains as objects shall define the scope of NEs. Operations shall not be performed on NEs not contained in domains.

At the OMWeb interface, the access control is based on users or groups and objects; and the security attribute object ID of an object must have a domain, including the specified NE, device type, and NEs in the subnet.

At the ManagementWeb and OMWeb interface, the access control is used to identify all the operations over objects through the MAE client if the operation rights have been assigned by the **SMManagers** or the super user **admin** (identification and authentication of operation rights)

(FDP_ACC.2, FDP_ACF.1, FMT_SMR.1, FMT_MSA.1, and FMT_MSA.3)

At the OMWeb interface, the MML commands defined by the managed NEs, are used to directly perform the operations on the corresponding NE through the channel between the NE and TOE. The access rights with MML command group (containing some MML commands) can be assigned to users and roles. The MML command groups are classified into System Command, Alarm Query, Alarm Management, Performance Query, Performance Management, Device Query, Device Management, Trace Query, Trace Management, Wireless Query, Wireless Management, Transport Query, Transport Management, Security Query, Sucurity Management, Time Query, Time Management, Software Query, Software Management, Test Query, Test Management, Fault Information Collection. The MML command access control is only used to identify the commands through the MML client function of the MAE client.

At the ManagementWeb and OMWeb interface, before any operations through the client of TOE, the access rights related with these operations shall be authenticated with the token of corresponding user session.

(FDP_ACC.2, FDP_ACF.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3)

7.1.4 IP-based ACL

At the ManagementWeb and OMWeb interface, the TOE can offer an access control list (ACL) of features based on IP addresses for controlling which terminals can access the TOE through the TOE client. The ACL is based on IP addresses. The security role **SMManagers** and the super user **admin** can specify each individual IP address or IP address range in the ACL of a specified user ID. The user can log in to the TOE only from terminals whose IP addresses are in the ACL.

(FMT_SMF.1 and FTA_TSE.1)

7.1.5 Communication Security

The TOE supports encrypted transmission between NEs and the TOE, the external system and the TOE, remote user and the TOE. It provides secure protocols, such as TLS, SNMPv3, SSHv2 and SFTP, for data transmission. The TOE integrates a private CA called LiteCA for issuing TLS certificates to internal services or NEs (FCS_COP.1.1/RSASSA, FCS_COP.1.1/ECDSA). The certificate key type can be either RSA (FCS_CKM.1.1/RSA) or ECDSA (FCS_CKM.1.1/ECDSA), (FCS_RBG.1 and FCS_RBG.2 provides the random number required by FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECDSA).

- Communication Security between NEs and the TOE:

As a client, the TOE can initiate SSHv2 and TLS connections to establish secure channels with the NEs.

As a server, the TOE also provides secure channels for the communication with NEs to perform performance data bulk collection and software backup and update. The secure channels are based on TLS connections initiated by NEs.

- Communication Security between the external system and the TOE:

As a client, the TOE can establish secure channels with the external system (like AAA server, syslog server) over TLS, SNMPv3, or SSH.

As a client, the TOE can initiate SSH connections to establish secure channels with the OSS, service orchestrator or service application.

As a server, the TOE can receive the TLS, HTTPS, and SNMPv3 connections initiated by the OSS, service orchestrator, or service application to establish secure channels.

The TOE supports communicating with a CA server to apply the certificates. To prevent modification, insertion and replay, the communication uses CMPv2 protocol over an HTTPS channel with RSA or ECDSA signature protection of the certificate. (FPT_ITI.1)

- Communication Security between remote users and the TOE:

The remote users access MAE through web portal by initiating HTTPS connections.

(FTP_TRP.1, FTP_ITC.1/NE, FTP_ITC.1/ External System)

- Communication Security inside the TOE:

  Services are accessed through the TLS security protocol. (FPT_ITT.1)

7.1.6 User Session Management

The TOE provides user session management. The TOE provides the following user session management at the ManagementWeb and OMWeb interface:

1. Session establishment

   The session will be established after successful login authentication. When more than three unsuccessful login attempts are detected since the last successful login, The TOE will generate an alarm. The session establishment will be denied based on the policy below (FTA.TSE.1).

   Upon successful session establishment, the TOE will display the welcome message, last successful login date, time and IP address, last unsuccessful login date, time and IP address, login failure times since last successful login (FTA_TAH.1).

2. TSF-initiated session Termination

   If a user does not perform any operation within the period of the default value 30 mins) specified by this parameter, the user will be logged out. The setting takes effect only for local and remote users and does not take effect for third-party users. If this parameter is set to Unlimited, user sessions will not be automatically logged off (FTA_SSL.3).

3. User-initiated session termination

   Login user can click the user name in the upper right corner of the page and choose Logout (FTA_SSL.4).

4. Users and their following security attributes:

   a. Time segment for login, which means that the user shall log in to the TOE within a specific time segment.

   b. ACL, addressed in the previous section.

   c. Maximum online sessions, which indicates that the number of online sessions shall not exceed the maximum sessions, otherwise the user login requests after the maximum online sessions shall be refused by the TOE. The default is none.

   d. Disabled status, which means the user cannot log in to the TOE in the disabled status.

5. System security policy, which is prior to the security attributes of individual users

   System login mode, which supports the multi-user login mode and single-user login mode. During system operation and maintenance, the single-user mode is recommended to prevent other users from logging in to the system and performing operations that may affect O&M efficiency. When the single-user login mode is selected, the TOE refuses all login requests including those for online sessions except that of the super user **admin**. The multi-user login mode is a normal mode and has no special limits.

7.1.7 Auditing

The TOE can generate audit records for security-relevant events as described in FAU_GEN.1. The audit record has the following information: the activity name, level, user ID, operation type, operation date and time, terminal, object, operation result, and details.

The audit review can be implemented with filter criteria on the MAE client by users attached to SMManagers, users with log query rights. Any user cannot delete and modify the audit records.

Conditions for dumping logs: The number of logs in the database exceeds 1 million, the size of the logs in the database exceeds 80% of the capacity, or the number of days for storing the logs exceeds 45 days. To ensure sufficient database space, the system checks logs every hour and saves logs that meet the requirements to the hard disk of a server. Then the dumped logs are automatically deleted from the database.

Conditions for deleting log files: The size of the log files is greater than 1024 MB (default value), the log files are stored for more than 45 days (default value), or the total number of log

files exceeds 1000 (default value). To ensure sufficient disk space, the system checks log files every hour and deletes log files meeting the requirements from the hard disk.

By default, a maximum of 1 million logs can be stored in the database. If the database space of log management is greater than or equal to 16 GB. The logs that exceed the maximum number of logs stored in the database will be dumped.

The values in the preceding log dump conditions are default values.

Log service start/stop of the O&M plane will be recorded in audit logs of the management plane. Log service start/stop of the management plane will be recorded in the /var/log/messages directory of the OS.

(FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.2, FAU_STG.4)

7.1.8 Security Management Function

The TOE provides security management if necessary. Only administrators have the privilege to manage the behaviors of TOE security functions. This is partially already addressed in more details in the previous sections of the TSS. It includes security attributes below.

1. Users and their following security attributes:
    a. User ID, which is a user identifier, defined as a username in the TOE.
    b. User Group, which is the same as a role definition.
    c. Password, which should meet the predefined password policy, is encrypted with PBKDF2 and stored in the database.
    d. Time segment for login, addressed in the previous section.
    e. ACL, addressed in the previous section.
    f. Maximum online sessions, addressed in the previous section.
    g. Disabled status, addressed in the previous section.
2. System security policy, which is prior to the security attributes of individual users
    a. System login mode, addressed in the previous section.
    b. Password policy, which has basic parameters and advanced parameters. Basic parameters include the following items: Min. Length of common user password, Min. Length of super user password, Max. Length of password, Max. Period for password repetition (months), Password validity period (days), Minimum validity period of the password (days), Number of days warning given before password expiry, The Password Cannot Be Similar to History Passwords. Advanced parameters include the following items: Min. Different characters between new and old passwords, Min. Letter, Min. Lowercase, Min. Numbers. Account policy, which has an upper threshold for legal login times and the excessive login attempts cause account locking. Super user **admin** is not allowed to be locked. All the users should meet the account policy defined in the TOE.

The TOE restricts the ability to manage the certificates, private keys, and symmetric keys to SMManagers and users with sufficient user permissions.

(FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_MOF.1, FMT_MTD.1)

7.1.9 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 AES256-GCM algorithm to protect sensitive data. (FCS_COP.1.1/SYM).
2. The TOE shall release the cryptographic key memory by overwriting the byte or char array with 0 if the key is no longer used (FCS_CKM.6.1/SYM, FCS_CKM.6.1/SIG, FCS_CKM.6.2).
3. The TOE supports a three-layer key management structure of root key, master key and working key. The root key is generated by PBKDF2 (HMAC-SHA2) algorithm from root key materials. The master key is generated with a 64-byte random number obtained from the TOE's deterministic random number, the master key is encrypted and protected by the root key. The working key is generated by PBKDF2 (HMACSHA2) algorithm from master key materials, the working key is encrypted and protected by the master key, the working key is used to provide confidential and complete protection for sensitive data saved in a local PC or data transferred through insecure channels. Both the two keys can be updated manually (FCS_CKM.1.1/PBKDF2), (FCS_RBG.1 and FCS_RBG.2 provides the random number required by FCS_CKM.1.1/PBKDF2).
4. The TOE supports hashing of data using PBKDF2 (SHA256) algorithm according to [RFC8018] for password hashing. The iteration number is at least 10,000 times. The salt used in PBKDF2 is a 16-byte random number obtained from the TOE's deterministic random number generator (FCS_COP.1.1/PBKDF2).
5. The TOE supports issuing certificates and can generate RSA, ECDSA key pairs according to the key generation algorithm described in (FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECDSA), (FCS_RBG.1 and FCS_RBG.2 provides the random number required by FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECDSA). Then, perform the corresponding digital signature operation according to the digital signature algorithm described in (FCS_COP.1.1/RSASSA and FCS_COP.1.1/ECDSA) to generate the certificate.
6. The TOE supports backup the symmetric encryption key.(FCS_CKM.3)

8 Abbreviations, Terminology and References

8.1 Abbreviations

Abbreviations	Full Spelling
AAA	Authentication Authorization Accounting
ACL	Access Control List
AOC	Agile Open Container
BSS	Business Support System
CA	Certificate Authority
CAS	Central Authentication Service
CC	Common Criteria
CHR	Call History Record
CMP	Certificate Management Protocol
CORBA	Common Object Request Broker Architecture
CSP	Cloud Service Provider
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
eNodeB	E-UTRAN NodeB
EPC	Evolved Packet Core
FTP	File Transfer Protocol

Abbreviations	Full Spelling
FTPs	FTP over SSL
GSM	Global System for Mobile Communications
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IMS	Information Management System
IdP	Identity Provider
LTE	Long term evolution
MAE	MBB Automation Engine
MBB	Mobile broadband
MML	Man-Machine Language
MR	Measurement Report
NE	Network Element
NGN	Next Generation Network
NMS	Network Management System
NTP	Network Time Protocol
NBI	Northbound Interface
OM	Operation and Maintenance
OSS	Operations Support System
PKI	Public Key Infrastructure
PP	Protection Profile
RAN	Radio Access Network
RAT	Radio Access Technology
REST	Representational State Transfer
SFR	Security Functional Requirement
SFTP	SSH File Transfer Protocol
SIG	LTE-cell-level signaling tracing messages of the medium depth for signaling correction
SNMP	Simple Network Management Protocol
SNMPv3	SNMP version 3
SSH	Secure Shell
SSHv2	SSH version 2

Abbreviations	Full Spelling
SSL	Security Socket Layer
SSO	Single Sign-on
ST	Security Target
STP	Signaling Transfer Point
SBI	Southbound Interface
SOP	Standard Operation Procedure
SDN	Software-defined Networking
SAML	Security Assertion Markup Language
SP	Service Provider
TCP	Transfer Control Protocol
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
PP	Protection Profile
UGW	User Gateway
USN	User Sequence Number
UMTS	Universal Mobile Telecommunications System
WCDMA	Wideband Code Division Multiple Access
WebNIC	Web Based Network Information Collection
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRAN	Wireless Regional Area Network
E2E	End to End
VM	Virtual Machine

8.2 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.

Terminology	Explanation

Terminology	Explanation
Administrator	An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition. From the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.
Operator	See User.
User	A user is a human or a product/application using the TOE.
Access Network	In telecommunications, an access network is a network that connects subscribers to telecommunication service providers over public ground. It can be considered the route between the subscriber's home and the ISP itself. The access network is composed of the carrier's station and the end user.
OM data	Data user for system operation and maintenance.
Access Domain	MAE provides the MAE-Access subsystem to connect to NEs to implement basic NE O&M, monitoring, and data openness.
Deploy Domain	MAE provides the MAE-Deployment subsystem including configuration solutions.
EVA Domain	MAE provides the MAE-Evaluation subsystem to implement network-level monitoring, network assessment topic, and network service provisioning assessment.
OPT Domain	MAE provides the MAE-Optimization subsystem to implement network self-optimization.
TSP Domain	This module provides network modeling data and generates enhanced functions such as geographic location and scenario identification based on the CHR/MR. This module provides an analysis and computing framework, supports codeless computing extension and plug-in computing extension based on the provided data model, and allows services to complete network-level and service-level analysis and computing.
TSF Domain	This module collects signaling data (CHR/MR) based on software, opens data to northbound systems and value-added domain systems, and allows service tools to obtain data. This module also provides the capabilities of NE-level data association analysis and processing in the northbound open scenario.

8.3 References

Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model

Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components

Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1, November 2022 — Evaluation methodology

