CC HUAWEI iMaster NCE Security Services Security Target

Version 2.4

Date 2026-10-23



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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 1

2 Introduction 3

2.1 ST Identification 3

2.2 TOE reference 3

2.3 TOE Overview 4

2.3.1 TOE Usage and Major Security Features 4

2.3.2 TOE Type 5

2.3.3 Required Non-TOE Hardware and Software 5

2.4 TOE Description 9

2.4.1 TOE Definition Scope 9

3 Conformance Claims 13

3.1 CC conformance claim 13

4 Security Problem Definition 14

4.1 Assumptions 14

4.2 Threats 15

4.2.1 Assets and Agents 15

4.2.2 Threats Addressed by the TOE 15

4.3 Organisational Security Policies 16

5 Security Objectives 17

5.1 Security Objectives for the TOE 17

5.2 Security Objectives for the Operational Environment 17

5.3 Security Objectives Rationale 18

5.3.1 Coverage 18

5.3.2 Threats Sufficiency 19

5.3.3 Assumptions sufficiency 20

6 Extended Components Definition 22

7 Security Requirements for the TOE 23

7.1 Conventions 23

7.2 Security Functional Requirements 23

7.2.1 Security Audit (FAU) 23

 Copyright © Huawei Technologies Co., Ltd.

7.2.2 User Data Protection (FDP) 26
7.2.3 Identification and Authentication (FIA) 27
7.2.4 Security Management (FMT) 30
7.2.5 TOE Access (FTA) 32
7.2.6 Trusted Path/Channels (FTP) 33
7.2.7 Cryptographic Support (FCS) 34
7.3 Security Functional Requirements Rationale 37
7.3.1 Coverage 37
7.3.2 Sufficiency 39
7.3.3 Security Requirements Dependency Rationale 41
7.4 Security Assurance Requirements 44
7.5 Security Assurance Requirements Rationale 45
8 TOE Summary Specification 46
8.1 TOE Security Functionality 46
8.1.1 User Management 46
8.1.2 Authentication 47
8.1.3 Access Control 48
8.1.4 Communication Security 49
8.1.5 User Session Management 49
8.1.6 Auditing 50
8.1.7 Security Management Functions 51
8.1.8 Cryptographic Functions 51
9 Abbreviations, Terminology and References 53
9.1 Abbreviations 53
9.2 Terminology 54
9.3 References 55

 Copyright © Huawei Technologies Co., Ltd.

1 About This Document

Change History

Version	Date	Change Description	Author
V1.0	2026-01-31	Initial Draft	Li Ling, chengyanbo
V1.1	2026-03-12	Modified according to review comments.	Li Ling
V1.2	2026-03-24	Modified according to review comments.	Li Ling
V1.3	2026-04-02	Modified according to review comments.	Li Ling
V1.4	2026-04-21	Modified the FCS part. Delete FCS_CKM.1/ECDSA，FCS_CKM.1/DH, FCS_COP.1/ECDSA. Add FCS_CKM.1/RSA, FCS_COP.1/RSA, FCS_COP.1/CHACHA	Li Ling
V1.5	2026-06-11	Modified according to review comments.	Li Ling
V1.6	2026-07-02	Modified according to review comments.	Li Ling
V1.7	2026-07-09	Modified according to review comments.	Li Ling
V1.8	2026-07-15	Modified according to review comments.	Li Ling
V1.9	2026-07-28	Modified according to review comments.	Li Ling
V2.0	2026-08-05	Modified according to review comments.	Li Ling
V2.1	2026-08-11	Modified according to review	Li Ling

 Copyright © Huawei Technologies Co., Ltd.

Version	Date	Change Description	Author
		comments.	
V2.2	2026-08-14	Modified according to review comments.	Li Ling
V2.3	2026-08-25	Modified according to review comments.	Li Ling
V2.4	2026-10-23	Modified according to review	Li Ling

2 Introduction

This Security Target is for the evaluation of HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100).

2.1 ST Identification

Title: CC HUAWEI iMaster NCE Security Services Security Target

Version: 2.4

Author: Huawei Technologies Co., Ltd.

Publication date: 2026-10-23

2.2 TOE reference

TOE name: HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100)

TOE version: V100R026C01SPC300

TOE Developer: Huawei Technologies Co., Ltd.

NOTE: in manufacture internal maintenance, HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100) refers to "CloudSOP". The name and version number of the TOE (CloudSOP) used in the deployment environment can be queried via the command line (Displayed as follows: CloudSOP V100R026C01SPC300).

VRC versions are defined as follows:

 Copyright © Huawei Technologies Co., Ltd.

- V version of the software and hardware platform hosting the TOE software. Thus, the TOE is implemented software part of a larger system, consisting of hardware and other none-TOE software.
- R version is released for customer at a specific time. It is a collection of features that is embodied in the form of a product.
- C version is the customized version developed based on the R version to fast meet customer demands.
- SPC version is the cold service patch version of the software.

2.3 TOE Overview

The TOE (CloudSOP) is a next-generation OSS platform focused on information and communications technology (ICT) integration. The TOE provides platform security capability components. Based on service requirements, service functions are further developed on the CloudSOP platform. Products developed based on the CloudSOP platform have the same security capability components.

The TOE can be deployed on NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (all V100R025C10SPC100), NCE-Campus(V300R025C10SPC100) and SecoManager (V500R25C10SPC100).

The TOE is a software-only TOE consisting of a single, cohesive software package designed to provide security services across multiple NCE products. NCE-FAN V100R025C10SPC100 is the reference product used for the evaluation of the TOE, and all security requirements defined in this ST are evaluated in this configuration.

The TOE Version V100R026C01SPC300 identifies the specific software build of the TOE as deployed on the reference product NCE-FAN V100R025C10SPC100. Although the TOE is identified by this specific version string, the security software component is architecturally identical and portable across the NCE product family.

2.3.1 TOE Usage and Major Security Features

The TOE is a unified platform that manages, controls, and maintains cloud-based SDN networks. It is a unified software orchestration and workflow engine that implements automation and autonomy, including planning and simulation, service provisioning, monitoring, assurance, and optimization, on physical and virtual networks throughout their lifecycles.

The major security features of TOE are:

1. User management
2. Authentication
3. Access control
4. Communication security
5. User session management
6. Auditing
7. Security management functions
8. Cryptographic functions

 Copyright © Huawei Technologies Co., Ltd.

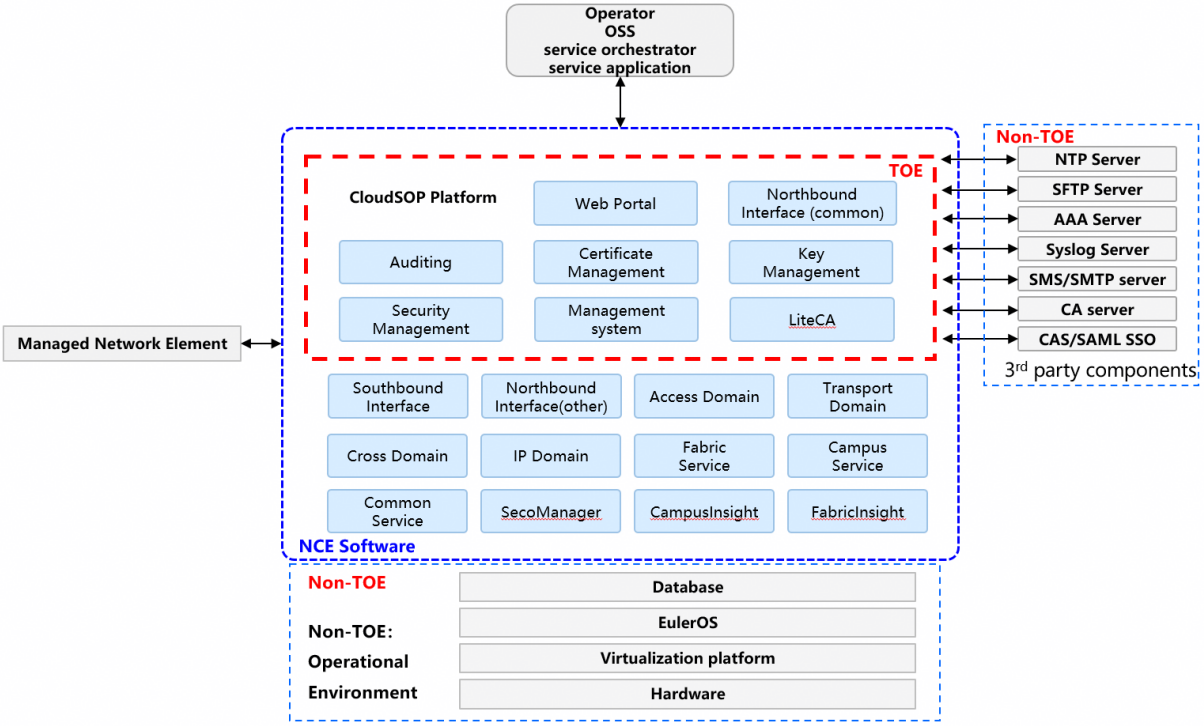
The detailed description of the security features above is in the 2.4.1.2 Logical Scope.

2.3.2 TOE Type

The TOE includes the security functions implemented by the CloudSOP platform, which are consistent for NCE products.

In the northbound direction, the TOE provides Web portals and northbound interfaces for O&M personnel, OSS, service orchestrator and service application. In the southbound direction, it provides some common configuration and management capabilities for Huawei network devices. The TOE also interconnects with external NTP servers, SFTP servers, AAA authentication servers, Syslog servers, CA servers, SMS/SMTP servers and CAS/SAML SSO.

Figure 2-1 TOE overview



Note: All security functional requirements defined in this ST are applicable to both the Management Plane and the O&M Plane as two independent, isolated functional instances.

2.3.3 Required Non-TOE Hardware and Software

The TOE cannot operate independently and requires the NCE platform for deployment. The TOE can be deployed on NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight, NCE-Campus and SecoManager. The TOE is the common part of all these products. To build each product, you add piece of software that realize the different products.

The TOE is a software component that relies on the iMaster NCE to operate. The following components are part of the Operational Environment and are NOT part of the TOE.

 Copyright © Huawei Technologies Co., Ltd.

2.3.3.1 NCE Business Components

The iMaster NCE product is logically divided into two parts:

1. The TOE (CloudSOP): Responsible for the security functions.
2. The Non-TOE Software (referred to as the NCE Business Components): Responsible for the general business logic and network management functions. And the connection to the NE is outside the TOE.

The NCE Business Components represent the software components of iMaster NCE that are excluded from the TOE boundary. The TOE interacts with the NCE Business Components via well-defined internal interfaces to provide security services. The NCE Business Components are considered part of the TOE's Environment.

The following lists the non-TOE software packages when it is deployed in NCE-FAN.

Software Package Name
iMasterNCE-FAN_V100R025C00SPC100_CommonService_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NBICommonService_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_ACFan_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_AOCCore_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_APaaSCore_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_APIDesigner_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_AutomationEngine_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_Basic_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_DataCubeCoreService_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_DigitalEngine_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_ExtAdvancedSEC_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_FanComSrvSolution_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_FanCommon_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_Infra_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_IntelligentPlat_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_LegacyCollector_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NCEPGW_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSAccess_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSBase_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSDC_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSNBI_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSPMS_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_NMSiMap_linux-aarch64.7z

 Copyright © Huawei Technologies Co., Ltd.

iMasterNCE-FAN_V100R025C00SPC100_NetworkDataIngestion_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_ProductSolution_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_TrustCenter_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_UniCollect_linux-aarch64.7z
iMasterNCE-FAN_V100R025C00SPC100_WorkFlowEngine_linux-aarch64.7z

2.3.3.2 Non-TOE hardware

Since the TOE is a software platform, its deployment depends on the deployment of the NCE product. We use NCE-FAN as its deployment environment.

We refer to *iMaster NCE-FAN V100R025C10 Server Hardware Specifications* to deploy the TOE environment.

Table 2-1 Hardware configurations

Hardware Type	Model	Requirements
512 GB server standard configuration	TaiShan 200 (Model 2280)	• CPU: 2 x Kunpeng 920 (2.6 GHz, 64 cores) • RAM: 16 x 32 GB DDR4 • Hard disk: 12 x 1200 GB SAS HDD or 10 x1920 GB SSD • RAID controller card: MegaRAID 9560-8i (4GB cache), Avago 3508 (2 GB cache), or PMC3152 (2 GB cache) • NIC: 2 x 4 GE electrical ports + 2 x 2 10GEoptical ports delivered, compatible with 2 x 4GE electrical ports + 2 x 2 10GE/25GE opticalports, 2 x 4 GE electrical ports + 2 x 4 10GE/25GE optical ports
10GE switch	CE6863H	• 10GE ports: 48 • 100GE ports: 6 • Version: V300R022C00
	CE6885	• 10GE ports: 48 • 100GE ports: 8 • Version: V300R023C00SPC500

Table 2-2 Server configuration requirements

Item	Type	Version
Delivered software	Virtualization software	FusionCompute (KVM) 8.10

 Copyright © Huawei Technologies Co., Ltd.

Item	Type	Version
configurations	OS	EulerOS V200R013
	Database	Gauss100 OLTP 1.11
		Redis 6.2.14

The NCE Operation System is excluded from the TOE physical boundary.

2.3.3.3 Operating Environment

Except the Server as described above, the environment also comprises the following components:

Table 2-3 Environment components

Component	Required/Optional	Usage/Purpose Description for TOE Performance
Network Elements (NEs)	Required	NEs that are managed by the TOE and support security communication protocols with the TOE.
Web portal	Required	The web portal connects to the TOE using HTTPS.
OSSs, service orchestrators and service applications	Required	The OSSs, service orchestrators and service applications that connect to the TOE through external interfaces like RESTful interfaces.
AAA server	Optional (Required in evaluation configuration)	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 (Required in evaluation configuration)	Syslog server used to transmit syslog messages.
SFTP server	Optional (Not required in evaluation configuration)	SFTP server used to upload performance files and back up NE data.
SMS/SMTP server	Optional (Not required in evaluation configuration)	TOE sends notifications by emails or messages.

 Copyright © Huawei Technologies Co., Ltd.

Component	Required/Optional	Usage/Purpose Description for TOE Performance
CA server	Optional (Not required in evaluation configuration)	CA server can apply for a certificate, update the certificate, and publish the certificate revocation list (CRL) file.
Other NCE acting as CAS/SAML SSO	Optional (Required in evaluation configuration)	Other NCE can be used as CAS/SAML SSO server for federated authentication. CAS/SAML SSOimplements SSO login based on CAS/SAML. It consists of a server and a client. The server serves the client to implement unified authentication. After logging in to the server, you can log in to the client without entering the user name and password again.
NTP server	Required	NTP server is used to sync the time of the TOE.

2.4 TOE Description

2.4.1 TOE Definition Scope

2.4.1.1 Physical Scope

The physical scope for the TOE is the source code of CloudSOP platform, which is compiled into multiple compressed packages for each scenario. The combination of all packages is the same TOE boundary for each scenario. However, there is no strict mapping regarding the packages within each scenario.

The CloudSOP platform provides service packages, and NCE will be built into release packages. As the TOE cannot be installed and run independently, the TOE deployment depends on NCE.

Huawei engineers assist users in logging in to the HUAWEI support website (https://support.huawei.com/carrier) and downloading the software packet 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).

TOE software package consists of binary compressed files. The following software packages and documents are required and are part of the TOE.As the TOE is contained within the NCE-FAN platform, the delivery process is performed through the NCE-FAN software packages. The TOE components are distributed across several NCE-FAN packages, and these packages may also include elements that are not part of the TOE. The table below identifies the software packages downloaded from the HUAWEI support website that contain TOE components (column “Release Software Package”), and for each of these packages specifies the elements that are part of the TOE (column “Included TOE Parts”).

 Copyright © Huawei Technologies Co., Ltd.

Table 2-4 TOE software list

Released Software Package	Sigature file	Included TOE parts
iMasterNCE-FAN_V100R025C00SPC100_OMP_linux-aarch64.zip	iMasterNCE-FAN_V100R025C00SPC100_OMP_linux-aarch64.zip.p7s	SM-26.455.703-euler_arm64.zip AuditLog-26.455.644-euler_arm64.zip CloudSOPJavaFrameworks-26.455.620-euler_arm64.zip MCTools-26.455.641-euler_arm64.zip
iMasterNCE-FAN_V100R025C00SPC100_SRM_linux-aarch64.7z	iMasterNCE-FAN_V100R025C00SPC100_SRM_linux-aarch64.7z.p7s	SMLogLic-26.455.994-euler_arm64.zip
iMasterNCE-FAN_V100R025C00SPC100_CloudSOPCloudService_linux-aarch64.7z	iMasterNCE-FAN_V100R025C00SPC100_CloudSOPCloudService_linux-aarch64.7z.p7s	MinApiMgr-26.455.690.zip
iMasterNCE-FAN_V100R025C00SPC100_CoreBase_linux-aarch64.7z	iMasterNCE-FAN_V100R025C00SPC100_CoreBase_linux-aarch64.7z.p7s	SnbCertMgmt-26.455.683-euler_arm64.zip

For product documentation, the TOE guide will be integrated into the product documentation. Please refer to the following:

Table 2-5 TOE guidance list

Name	Version
iMaster NCE V100R025C10 Product Documentation (Project Deployment & System Maintenance, Arm)	02
iMaster NCE-FAN V100R025C10 Product Documentation	02
CC HUAWEI NCE Security Services AGD_PRE	1.5
CC HUAWEI NCE Security Services AGD_OPE	1.9

Info:

 Copyright © Huawei Technologies Co., Ltd.

Users can login the HUAWEI support website to read all the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.

2.4.1.2 Logical Scope

The major security features of the TOE 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. On the management plane, it has the default user groups including Administrators, SMManagers, Monitors and Operators, while on the O&M plane, it has the default user groups like Administrators, SMManagers, NBI User Group, Maintenance Group, Operator Group. 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 on the management plane, the O&M plane. The TOE optionally provides authentication credentials obtained from an external AAA in the IT environment on the O&M plane.

Access Control

The TOE supports admin and 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.

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

Communication Security

The TOE supports encrypted transmission within the TOE server, between a browser and the TOE server, and between an OSS/service orchestrator/service application and the TOE 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 logs for security-relevant management and stores the logs in the database. Logs record routine maintenance events of the TOE. For security purposes, the TOE provides security logs, operation logs and system 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 configurations, such as modification of IP addresses and addition of services.

 Copyright © Huawei Technologies Co., Ltd.

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

The query and filter functions are provided on the graphical user interface of the NCE Client, 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 Functions

Cryptographic functions are dependencies required by security features. The TOE supports cryptographic algorithms as described in section 7.2.7 Cryptographic Support.

 Copyright © Huawei Technologies Co., Ltd.

3 Conformance Claims

3.1 CC conformance claim

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

This ST is EAL3 augmented with ALC_FLR.2.

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

No conformance to a Protection Profile is claimed.

 Copyright © Huawei Technologies Co., Ltd.

4 Security Problem Definition

4.1 Assumptions

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

A.PhysicalProtection It is assumed that the TOE and its operating environment(i.e. the complete system including the device hardware and attached peripherals) are properly protected to prevent unauthorized physical access. It is assumed that only Administrators and non-Administrators with explicit approval by the Administrator(s) are authorized to physically access the TOE and its operational environment. The underlying hardware and firmware that support the running of the TOE are trusted and can support the secure running of the TOE.

A.NetworkSegregation It is assumed that the network interfaces of the server and TOE clients will be accessed only through the subnet where the TOE host is installed. The subnet is separated from the public network.

A.AdministratorBehaviour It is assumed that the super user admin, a user that belongs to the SMManagers and Administrators groups and the users of the underlying operating system and operators authorized by the administrator to perform security-related operations will behave correctly and will not perform any harmful operation on the TOE.

A.NTP It is assumed that operating environment will provide an accurate time source, in order to ensure normal operations of the TOE.

A.NetworkElements It is assumed that the managed network elements are trusted and can support the Security connection with the TOE.

A.Components It is assumed that the 3rd party components (NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, CA server and CAS/SAML SSO) are considered trusted and will not attack the TOE. For RADIUS authentication deployments, it is assumed that the RADIUS server supports the reception and processing of fragmented RADIUS authentication requests.

It is assumed that the OSS/Service Orchestrator/Service application are considered trusted and will not attack the TOE.

It is assumed that the NCE Client are considered trusted and will not attack the TOE.

A.TrustedPlatform It is assumed that the platform including EulerOS, GaussDB, hardware and virtual machine used by the TOE is trusted, and is properly hardened by the

 Copyright © Huawei Technologies Co., Ltd.

Administrator of the customer with administrator rights. The platform provides a security domain for the TOE free from tampering by other programs on the same platform.

4.2 Threats

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

4.2.1 Assets and Agents

Table 4-1 TOE Assets

Asset	Description
TOE security function (TSF) data	The integrity and confidentiality of TSF data (such as user account information, passwords and audit logs) should be protected against threat agents.
O&M data	The confidentiality and integrity of the O&M 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

Table 4-2 T.UnauthenticatedAccess

Threat: T.UnauthenticatedAccess	
Attack	An unauthenticated person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
Asset	TSF and O&M data
Agent	An attacker

 Copyright © Huawei Technologies Co., Ltd.

4.2.2.2 T.UnauthorizedAccess

Table 4-3 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 O&M data. The user also performs unauthorized operations on NEs through the TOE.
Asset	TSF and O&M data
Agent	An unauthorized user

4.2.2.3 T.Eavesdrop

Table 4-4 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 NCE Client and TOE, and between the TOE and OSS/service orchestrator/service application.
Asset	TSF and O&M data
Agent	An eavesdropper

4.3 Organisational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Since the entire motivation for the defined security functionality is based on countermeasures against explicitly listed threats, no OSPs are defined.

 Copyright © Huawei Technologies Co., Ltd.

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 to secure network communication with the OSS, service orchestrator, service application, NCE client, third party components and non-TOE NCE component.
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 ACL policies to restrict user session establishment.
4. **O.Audit** The TOE provide functionality to generate audit data and logs for security-relevant administrative actions and user log in and log out activities. Post-event tracing is critical, and logging allows tracing attack paths, identify attackers, assess impact, and improve security measures.
5. **O.SecurityManagement** The TOE should provide the function of managing the security functions of the TOE. Users can manage the security functions of the TOE, including user management and configuration management.

5.2 Security Objectives for the Operational Environment

1. **OE.PhysicalProtection** The TOE is protected against unauthorized physical access. The operational environment protects the database against unauthorized physical access and data file damage.

   The operational environment shall protect the platform of the server that the TOE is running on, the hardware, infrastructure, and components that host and store the data, including the storage devices and servers where the database files are stored, the NCE client, the 3rd party components and TOE itself against unauthorized physical access.
2. **OE.NetworkSegregation** The operational environment protects the network where the TOE hosts are installed by separating it from the application (or public) network.

 Copyright © Huawei Technologies Co., Ltd.

3. **OE.AdministratorBehaviour** The super user admin, the users who belong to the SMManagers and Administrators groups, the Operators authorized by the administrator to perform security-related operations and the users of the underlying operating system will behave correctly and will not perform any harmful operation on the TOE.
4. **OE.NTP** The operational environment provides an accurate time source, in order to ensure normal operations on the TOE server.
5. **OE.NetworkElements** The operational environment ensures that the trusted NEs support the security connection with the TOE and private interface defined by Huawei.
6. **OE.Components** The 3rd party components are considered trusted and will not attack the TOE. The administrator shall ensure the communication between the TOE and the NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, CA server, and CAS/SAML SSO is secured when these servers are used. When RADIUS authentication is used, the Operational Environment shall provide a RADIUS server capable of receiving and processing fragmented RADIUS authentication requests.

   The OSS/Service Orchestrator/Service application and the NCE Client are considered trusted and will not attack the TOE.
7. **OE.TrustedPlatform** The operation environment provides a trusted platform like EulerOS, GaussDB, hardware, virtual machine and 10GE switch. The platform provides a security domain for the TOE free from tampering by other programs on the same platform. The Operational Environment shall provide a certified cryptographic library (e.g., OpenSSL) that performs self-tests to ensure the correct operation of the Random Bit Generator (RBG) and ensures that any failure of the RBG does not result in the leakage of sensitive data.

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 counters at least one threat.

Table 5-1 Mapping of security objectives to threats

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 counters at least one threat or assumption.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-2 Mapping of security objectives for the environment to assumptions and threats

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

5.3.2 Threats 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:

Table 5-3 Mapping of threats to security objectives

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 and IP address-based ACL policies for its users (O.Authentication). Authentication mechanisms can be configured by users with sufficient permissions (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit). And the threat is countered by requiring the TOE and database to implement an authentication mechanism for its users (OE.PhysicalProtection).
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 logs showing that if someone indeed performs unauthorized operations, they

 Copyright © Huawei Technologies Co., Ltd.

Threat	Rationale for Security Objectives
	can be traced to (O.Audit).
T.Eavesdrop	The threat of eavesdropping is countered by requiring security communications: - Securing network communication between the portal and TOE server over HTTPS (O.Communication). - Over security channels between the TOE server and the OSS/service orchestrator/service application (O.Communication). Management of secure communication channels can be performed by users with sufficient permissions (O.SecurityManagement).

5.3.3 Assumptions sufficiency

The following rationale justifies that security objectives for the operational environment can uphold each individual assumption and that the achievement of each security objective can contribute to the uphold of a specific assumption:

Table 5-4 Mapping of assumption to environment security objectives

Assumption	Rationale for Security Objectives
A.PhysicalProtection	The assumption of adequate physical protection is addressed by requiring the operational environment to protect the TOE, the platform on which it runs, the database, storage devices, the NCE client, and the third-party components against unauthorized physical access (OE.PhysicalProtection). This objective ensures that only authorized personnel can physically access the TOE and its supporting environment, thereby preserving the confidentiality and integrity of TSF and O&M data and supporting the secure operation of the TOE.
A.NetworkSegregation	The assumption that the TOE is deployed in a segregated subnet is addressed by requiring the operational environment to separate the network where the TOE hosts are installed from the application or public network (OE.NetworkSegregation). This objective reduces exposure of TOE interfaces to untrusted networks and helps maintain a controlled management environment consistent with the assumption.
A.AdministratorBehaviour	The assumption that privileged users and authorized operators behave correctly and do not misuse the TOE is addressed by the operational environment objective OE.AdministratorBehaviour. This objective requires the admin user, the users in the SMManagers and Administrators groups, the operators authorized by the administrator, and the underlying operating system users to act in a trustworthy manner and

 Copyright © Huawei Technologies Co., Ltd.

Assumption	Rationale for Security Objectives
	refrain from harmful actions, thereby supporting secure administration of the TOE.
A.NTP	The assumption that an accurate time source is available is addressed by OE.NTP, which requires the operational environment to provide an accurate time source for the TOE server. This supports correct time synchronization for the TOE and enables normal operation of time-dependent functionality such as audit logging and session control.
A.NetworkElements	The assumption that managed network elements are trusted and support secure connections with the TOE is addressed by OE.NetworkElements. This objective requires the operational environment to ensure that trusted NEs support the secure connection with the TOE and the Huawei-defined private interface, so that communications with managed devices can be established and maintained consistently with the assumption.
A.Components	The assumption that third-party components, OSS/service orchestrators/service applications, and the NCE client are trusted and do not attack the TOE is addressed by OE.Components. This objective requires the operational environment to treat these components as trusted and to ensure that communications between the TOE and external servers such as the NTP, SFTP, AAA, syslog, SMS/SMTP, CA, and CAS/SAML SSO servers are secured when used, thereby maintaining the trusted external environment assumed by the ST.
A.TrustedPlatform	The assumption that the TOE runs on a trusted and properly hardened platform is addressed by OE.TrustedPlatform. This objective requires the operational environment to provide a trusted platform including EulerOS, GaussDB, hardware, virtual machine, and 10GE switch, and to ensure that this platform provides a security domain for the TOE free from tampering by other programs on the same platform. It also requires the environment to provide a certified cryptographic library that performs self-tests and handles RBG failures securely, thereby supporting the trusted execution environment assumed for the TOE.

 Copyright © Huawei Technologies Co., Ltd.

6 Extended Components Definition

There is no extended component defined.

7 Security Requirements for the TOE

7.1 Conventions

The following conventions are used for the completion of operations:

- Strikethrough indicates text removed as a refinement
- underlined text 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.
- Allows a SFR to be used more than once with varying operations. SFRs are distinguished by.
- **Iteration:** Allows a SFR to be used more than once with varying operations. SFRs are distinguished by adding a string starting with "/" (i.e. 'FCS_COP.1/SYM').

7.2 Security Functional Requirements

7.2.1 Security Audit (FAU)

7.2.1.1 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;

c) **[The following auditable events:**

1. **User login and logout**
2. **User account management**
   a) **Creating, deleting, modifying and disabling 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**
   i. **Kicking out user sessions**
6. **ACL management**
   a) **Creating, deleting, and modifying ACLs**
   b) **Specifying ACLs for individual user account.**
7. **Management plane: operation set management; O&M plane: 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**].

7.2.1.2 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.

7.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1

The TSF shall provide [**users attached to admin and SMManagers, users with log query rights**] with the capability to read [**security logs, operation logs, system logs**] from the audit data.

FAU_SAR.1.2

The TSF shall provide the audit data 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

7.2.1.4 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.

7.2.1.5 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**].

7.2.1.6 FAU_STG.1 Audit data storage location

FAU_STG.1.1

The TSF shall be able to store generated audit data on the [***TOE itself, transmit***

the generated audit data to an external IT entity using a trusted channel according to FTP_ITC].

7.2.1.7 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.

 Copyright © Huawei Technologies Co., Ltd.

7.2.1.8 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 then remove the exported data from the database]** 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 90 days]**.

7.2.2 User Data Protection (FDP)

7.2.2.1 FDP_ACC.2 Complete Access Control

FDP_ACC.2.1

The TSF shall enforce the [**access control policy**] on [**subjects: users; objects: TOE application set and NEs**] 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.

7.2.2.2 FDP_ACF.1 Security Attribute-Based Access Control

FDP_ACF.1.1

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

1. **Users and their following security attributes:**
   a. **User ID**
   b. **User type**
   c. **User role assignment**
2. **TOE application sets, NEs, and the following security attributes:**
   a. **Application Operation Identification**
   b. **NE ID**]

Application Note:

The NE ID is a UUID automatically generated by the TOE when a NE is created. It has no business meaning and cannot be modified after creation.

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 when the user's roles have the corresponding permissions can perform the operations.**
2. **Users can be configured with different user role to control the access permission.**
3. **An operation set contains many operation rights that are assigned to specific user roles.**]

 Copyright © Huawei Technologies Co., Ltd.

FDP_ACF.1.3

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

FDP_ACF.1.4

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

7.2.3 Identification and Authentication (FIA)

7.2.3.1 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 TSF-mediated actions on behalf of that user.

7.2.3.2 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.

7.2.3.3 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, the local password authentication mechanism is used for user authentication, including authentication on the web interface and northbound interfaces.**
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 SSO authentication is enabled, user authentication is implemented by a remote CAS server.**
5. **When SAML SSO authentication is enabled, user authentication is implemented by a remote SAML server.**

Application Note:

CAS 2.0 references: https://apereo.github.io/cas/7.0.x/protocol/CAS-Protocol.html#20

SAML 2.0 references: https://apereo.github.io/cas/development/authentication/Configuring-SAML2-Authentication.html

7.2.3.4 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions [**changing the password**].

7.2.3.5 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.

Application Note:

The TSF will return an obscured username or password error when login failed, you cannot tell whether the username is wrong or the password is incorrect.

7.2.3.6 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. **Account enable status**
6. **Login time policy**
7. **Client IP address policy**
8. **User role assignment**
9. **Compulsory password renewal (Password validity period (days), In advance warning before password expires (days)**].

7.2.3.7 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 user account or IP address in accordance with the table below**].

 Copyright © Huawei Technologies Co., Ltd.

Table 7-1 User roles' default lockout duration

User roles	O&M Plane (by default)	Management Plane (by default)
Administrators both on the management and O&M plane	30 minutes	30 minutes
SMManagers both on the management and O&M plane	30 minutes	30 minutes
Monitors only on the management plane		30 minutes
Operators only on the management plane		30 minutes
NBI User Group only on the O&M plane	30 minutes	
Guests only on the O&M plane	30 minutes	
Maintenance Group only on the O&M plane	30 minutes	
Operator Group only on the O&M plane	30 minutes	

7.2.3.8 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(default 8, configuration range: 8-128)**
2. **Min. system administrator password length(default 8, configuration range: 8-128)**
3. **Max. password length(default 32, configuration range: 8-128)**
4. **Minimum number of positions with a character different between the old and new password (default 3, configuration range: 3-64)**
5. **Min. number of letters(default 2, configuration range:0-64)**
6. **Min. number of uppercase letters(default 1, configuration range:0-64)**
7. **Min. number of lowercase letters(default 1, configuration range:0-64)**
8. **Min. number of digits(default 1, configuration range:0-64)**
9. **Min. number of special characters(default 1, configuration range:0-64)**
10. **Password that cannot contain its username in reverse order**
11. **Policy that the password cannot contain repeated character sequences**
12. **Password that cannot contain user's mobile number or email address**

]

Application Note:

The defined quality metrics are configurable by the administrator.

 Copyright © Huawei Technologies Co., Ltd.

7.2.4 Security Management (FMT)

7.2.4.1 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 Policy**
10. **Login time policy**
11. **Configuration of the time interval of user inactivity for terminating an interactive session**
12. **Configuration of trusted channels for connecting to the external entities**

].

7.2.4.2 FMT_SMR.1 Security Roles

FMT_SMR.1.1

The TSF shall maintain the roles: [

1. **Administrators on the management plane**
2. **SMManagers on the management plane**
3. **Monitors on the management plane**
4. **Operators on the management plane**
5. **Administrators on the O&M plane**
6. **SMManagers on the O&M plane**
7. **NBI User Group only on the O&M plane**
8. **Guests only on the O&M plane**
9. **Maintenance Group only on the O&M plane**
10. **Operator Group only on the O&M plane**
11. **User-defined User Group].**

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

7.2.4.3 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [***determine the behavior 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	Plane
Administrators	Certificate management Configuration of trusted channels for connecting to the external entities NE management	O&M plane
Administrators	Certificate management Configuration of trusted channels for connecting to the external entities	management plane
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	O&M plane management plane
NBI User Group	Configuration of trusted channels for connecting to the external entities	O&M plane
Guests	Granted by SMManagers	O&M plane
Maintenance Group	NE Management Configuration of trusted channels for connecting to the external entities	O&M plane
Operator Group	NE Management Configuration of trusted channels for connecting to the external entities	O&M plane
Monitors	The user group has permission to monitor non-security operations	management plane
Operators	The user group has permission to perform non-security operations	management plane

 Copyright © Huawei Technologies Co., Ltd.

Role Name	Security Functions	Plane
user-defined User Group	Granted by SMManagers	O&M plane

7.2.4.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1

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

7.2.4.5 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1

The TSF shall enforce the [**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**].

7.2.4.6 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1

The TSF shall enforce the [**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.

7.2.5 TOE Access (FTA)

7.2.5.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1

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

1. **User identity (username and password)**
2. **Client IP address policies (IP address range for login)**
3. **Login time policies (limited time segment for account login)**
4. **User lock status and enablement status**
5. **Password validity period (days)**
6. **Maximum online sessions**

7. **Auto-logout time interval**]

7.2.5.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1

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

7.2.5.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

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

7.2.5.4 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.

7.2.6 Trusted Path/Channels (FTP)

7.2.6.1 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*].**

Application Note:

 Copyright © Huawei Technologies Co., Ltd.

Remote users can log in to TOE using a browser using HTTPS.

7.2.6.2 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

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

FTP_ITC.1.2

The TSF shall permit **[*the TSF and (the external system including the OSS, service orchestrator, service application, non-TOE NCE components 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 **[Interconnection with OSS/service orchestrators, service applications, non-TOE NCE components and third-party components]**.

7.2.7 Cryptographic Support (FCS)

7.2.7.1 FCS_CKM.1/PBKDF2 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]**

7.2.7.2 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA]** and specified cryptographic key sizes **[3072 bits]** that meet the following: **[FIPS 186-5]**.

7.2.7.3 FCS_CKM.1/ECDH Cryptographic key generation

FCS_CKM.1.1/ECDH

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Elliptic curve-based key establishment schemes]** and specified cryptographic key sizes **[256 bits, 384 bits, 521 bits]** that meet the following: **[NIST SP800-56A]**.

 Copyright © Huawei Technologies Co., Ltd.

7.2.7.4 FCS_CKM.1/ECDSA Cryptographic Key Generation

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, 384 bits, 521 bits]** that meet the following: **[FIPS 186-5]**

7.2.7.5 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1

The TSF shall perform [**read/write access to the cryptographic key internal copy**] in accordance with a specified cryptographic key access method [**encrypted by the encryption key specified by the user**] that meets the following: [**none**].

7.2.7.6 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1

The TSF shall destroy **[encryption 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: **[NIST SP 800-57 Part 1 Rev.5].**

7.2.7.7 FCS_COP.1/SYM 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, NIST SP 800-38D]**

7.2.7.8 FCS_COP.1/PBKDF2 Cryptographic operation

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].**

 Copyright © Huawei Technologies Co., Ltd.

7.2.7.9 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1/RSA

The TSF shall perform **[Digital signature]** in accordance with a specified cryptographic algorithm **[RSASSA-PKCS1-v1.5]** and cryptographic key sizes **[3072bits]** that meet the following: **[FIPS 186-5].**

7.2.7.10 FCS_COP.1/CHACHA Cryptographic operation

FCS_COP.1.1/CHACHA

The TSF shall perform **[symmetric decryption and encryption]** in accordance with a specified cryptographic algorithm **[CHACHA20-POLY1305]** and cryptographic key sizes **[256 bits]** that meet the following: **[RFC 8439]**.

7.2.7.11 FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA

The TSF shall perform **[hashing]** in accordance with a specified cryptographic algorithm **[SHA256, SHA384**] and cryptographic key sizes **[of none]** that meet the following: **[FIPS 180-4].**

7.2.7.12 FCS_COP.1/ECDSA Cryptographic operation

FCS_COP.1.1/ECDSA

The TSF shall perform **[Digital signature]** in accordance with a specified cryptographic algorithm **[ECDSA]** and cryptographic key sizes **[256 bits, 384 bits, 521 bits]** that meet the following: **[FIPS 186-5].**

7.2.7.13 FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.1.1

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

FCS_RBG.1.2

The TSF shall use a [***TSF noise source [/dev/random]***] for initialized seeding.

FCS_RBG.1.3

The TSF shall update the RBG state by [***reseeding***] using a [***TSF noise source [/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**].

 Copyright © Huawei Technologies Co., Ltd.

7.2.7.14 FCS_RBG.3 Random bit generation (internal seeding – single source)

FCS_RBG.3.1

The TSF shall be able to seed the RBG using a [***TSF hardware-based noise source]***[**/dev/random**] with a minimum of [**256**] bits of min-entropy.

7.3 Security Functional Requirements Rationale

7.3.1 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.1	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
FIA_UAU.7	O.Authentication

 Copyright © Huawei Technologies Co., Ltd.

Security Functional Requirements	Objectives
FIA_ATD.1	O.SecurityManagement O.Authentication O.Authorization
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 O.SecurityManagement
FMT_MSA.3	O.Authorization O.SecurityManagement
FTA_TSE.1	O.Authentication
FTA_SSL.3	O.Authentication O.SecurityManagement
FTA_SSL.4	O.Authentication
FTA_TAH.1	O.Authentication
FTP_TRP.1	O.Communication
FTP_ITC.1	O.Communication
FCS_CKM.1/PBKDF2	O.Communication
FCS_CKM.1/RSA	O.Communication
FCS_CKM.1/ECDH	O.Communication
FCS_CKM.1/ECDSA	O.Communication
FCS_CKM.3	O.SecurityManagement
FCS_CKM.6	O.Communication O.SecurityManagement

Security Functional Requirements	Objectives
FCS_COP.1/SYM	O.SecurityManagement
FCS_COP.1/PBKDF2	O.Authentication O.SecurityManagement
FCS_COP.1/RSA	O.Communication
FCS_COP.1/SHA	O.Communication
FCS_COP.1/CHACHA	O.Communication
FCS_COP.1/ ECDSA	O.Communication
FCS_RBG.1	O.Communication O.SecurityManagement
FCS_RBG.3	O.Communication O.SecurityManagement

7.3.2 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.Communication	Communication security is implemented by trusted channels (FTP_ITC.1, FCS_CKM.1/RSA, FCS_CKM.1/ECDH, FCS_CKM.1/ECDSA, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/CHACHA, FCS_COP.1/ECDSA, FCS_CKM.6) between TOE and external servers, and (FTP_TRP.1) between TOE and the NCE client. FCS_CKM.1/PBKDF2 generates the cryptographic keys used to protect data transmitted through insecure channels. FCS_RBG.1 and FCS_RBG.3 provide the random numbers required by FCS_CKM.1/*. Performance and inventory text files are transmitted to the OSS/service orchestrator/service application. (FTP_TRP.1) Management functionality to configure the trusted channel for NE communication is provided in (FMT_SMF.1).
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 TOE 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

Security objectives	Rationale
	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 TOE for multiple consecutive times, the locking policy for the account and IP address is executed (FIA_AFL.1).
O.Authentication	User authentication (including re-authentication) is implemented by (FIA_UAU.2, FIA_UAU.5, FIA_UAU.6) and supported by 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). Users can also terminate their own interactive sessions (FTA_SSL.4). 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 FCS_COP.1/PBKDF2. The authentication mechanism for NBIs and NEs to connect to TOE is also implemented by FIA_UAU.2.
O.Audit	The generation of audit logs is implemented by (FAU_GEN.1). Audit logs are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the identification mechanism (FIA_UID.2). Audit logs 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 logs are stored in the database, and exported into a file if the size of the audit log occupies over the configured maximum size (FAU_STG.1, FAU_STG.2, FAU_STG.4).
O.SecurityManagement	Management functionality is provided in (FMT_SMF.1/FIA_ATD.1/FIA_SOS.1/FMT_SMF.1/FMT_MOF.1/ FMT_MTD.1/FTA_SSL.4/FTA_SSL.3/ FMT_MSA.1/FMT_MSA.3). FCS_RBG.1 and FCS_RBG.3 provide the random numbers required by the TOE's cryptographic key generation mechanisms. 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) The irreversible encryption algorithms PBKDF2 are used to protect web user passwords. (FCS_COP.1/PBKDF2) The AES algorithm is used to encrypt service data (such as

 Copyright © Huawei Technologies Co., Ltd.

Security objectives	Rationale
	configuration data). (FCS_COP.1/SYM)

7.3.3 Security Requirements Dependency Rationale

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

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

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

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.2 (Hierarchical to FIA_UID.1)
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
FAU_STG.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 (Hierarchical to FDP_ACC.1) FMT_MSA.3
FIA_UID.2	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (Hierarchical

Security Functional Requirement	Dependencies	Resolution
		to FIA_UID.1)
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (Hierarchical to FIA_UAU.1)
FIA_ATD.1	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (Hierarchical to FIA_UAU.1)
FIA_SOS.1	None	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (Hierarchical to 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 (Hierarchical to FDP_ACC.1) 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	None	None
FCS_CKM.1/PBKDF2	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] FCS_CKM.3	FCS_COP.1/PBKDF2 FCS_CKM.3 FCS_CKM.6

Security Functional Requirement	Dependencies	Resolution
	[FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_RBG.1
FCS_CKM.1/RSA	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1/RSA FCS_CKM.3 FCS_CKM.6 FCS_RBG.1
FCS_CKM.1/ECDH	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1/SHA FCS_CKM.3 FCS_CKM.6 FCS_RBG.1
FCS_CKM.1/ECDSA	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1/ECDSA FCS_CKM.3 FCS_CKM.6 FCS_RBG.1
FCS_CKM.3	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5]	FCS_CKM.1/PBKDF2
FCS_CKM.6	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/PBKDF2
FCS_COP.1/SYM	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1/PBKDF2 FCS_CKM.3
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1/PBKDF2 PBKDF2 is a kind salting hash mechanism for storing passwords. There is not any key involved neither destroyed and the stored salted passwords do not require secure destruction.
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1/RSA FCS_CKM.3
FCS_COP.1/SHA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1/ECDH FCS_CKM.3
FCS_COP.1/CHACHA	[FDP_ITC.1, or FDP_ITC.2, or	FCS_CKM.1/RSA

 Copyright © Huawei Technologies Co., Ltd.

Security Functional Requirement	Dependencies	Resolution
	FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.3
FCS_COP.1/ECDSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1/ECDSA FCS_CKM.3
FCS_RBG.1	[FCS_RBG.3, or FCS_RBG.3] FPT_FLS.1 FPT_TST.1	FCS_RBG.3 FPT_FLS.1 and FPT_TST.1 are satisfied by OE. The TOE relies on OpenSSL's native Power-Up Self-Tests (POST) and Health Tests as defined in NIST SP 800-90A. These tests are performed by the library within the Operational Environment and satisfy the intent of self-testing. OpenSSL and the OS kernel return error codes upon RBG failure (e.g., entropy exhaustion). The TOE is designed to catch these errors and abort cryptographic operations, thus preserving a secure state.
FCS_RBG.3	FCS_RBG.1	FCS_RBG.1

7.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 augmented with ALC_FLR.2, as specified in [CC] Part 3. The following table provides an overview of the assurance components that form the assurance level for the TOE.

Table 7-2 Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design

 Copyright © Huawei Technologies Co., Ltd.

Assurance class	Assurance components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	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.2 Vulnerability analysis

7.5 Security Assurance Requirements Rationale

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

Dependencies within the EAL package selected (EAL3 augmented with ALC_FLR.2) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

 Copyright © Huawei Technologies Co., Ltd.

8 TOE Summary Specification

8.1 TOE Security Functionality

8.1.1 User Management

The TOE supports user management. User management involves user permission management, region management, and user maintenance and monitoring. Newly created users are not bound to any role by default, so they have no permissions. Users with the **SMManagers** role 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.

SMManagers 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.

The management plane is responsible for managing products, such as installation, deployment, upgrade, and backup and restoration. The management plane does not manage NEs. Therefore, the management plane provides only application permissions. 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.

On the O&M plane, 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. 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.

On every plane, there is a default and super user **admin**. On the management plane, the super user **admin** is bound to the **Administrators** and **SMManagers** roles on the management plane declared in FMT_SMR.1. On the O&M plane, the super user admin is bound to the **Administrators** and **SMManagers** roles on the O&M plane declared in FMT_SMR.1. This account has the permission to perform all functions in FMT_SMF.1.

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

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

 Copyright © Huawei Technologies Co., Ltd.

Role Name	Description
Administrators	Users attached to this role have permission to perform operations except managing users, querying security logs, querying personal security logs, and viewing online users.
SMManagers	Users attached to this role have permission to manage users, query security logs, and view online users.
Monitors	Users attached to this role have permission to monitor operations of the backup and restore, deployment, system monitoring, maintenance, system settings, and alarms.
Operators	Users attached to this role have permission to perform operations of the backup and restore, deployment, system monitoring, maintenance, system settings, and alarms.

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

Role Name	Description
Administrators	The user group has all the permissions except User Management, Query Security Log, View Online Users, and Query Personal Security Log.
SMManagers	The user group has the User Management, License Management, View Online Users, and Query Security Log permissions.
NBI User Group	The user group has the permission to configure the northbound interfaces such as CORBA, XML, TEXT and RESTful NBIs.
Guests	The domain of this user group is All Objects, and it has operation rights for default monitor operation sets. They can perform query operations, such as querying statistics, but cannot create or configure objects.
Maintenance Group	The domain of this user group is All Objects, and it has operation rights for default maintenance operation sets. In addition to the rights of Guests and Operator Group, users in this group have the rights to create services and perform configurations that affect the running of TOE and NEs.
Operator Group	The domain of this user group is All Objects, and it has operation rights for default operator operation sets. In addition to the rights of Guests group, users in this group have the rights to modify (rights to perform potentially service-affecting operations are not involved). For example, they can change alarm severities.

8.1.2 Authentication

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

 Copyright © Huawei Technologies Co., Ltd.

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 TOE will refuse the login request, the user must request the administrator to reset the password, the administrator can deactivate the password expiration policy (FIA_UAU.2).

The TOE shall verify that the password meets the password policies in FIA_SOS.1.1 which are configurable by the administrator (FMT_MSA.1, FMT_MSA.3 and FIA_SOS.1).

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(FIA_ATD.1).

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

If you enter the password for the admin user incorrectly for five consecutive times within 10 minutes, the client IP address will be locked for 10 minutes. 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. 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 and FTA_TSE.1).

The management plane supports local authentication and remote authentication. On the O&M plane, 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 O&M plane supports Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial In User Service (RADIUS) for AAA authentication. The O&M plane supports CAS and SAML SSO. SSO configuration allows users to access multiple mutually trusted application systems after only one login authentication. For supporting the SAML SSO, the O&M plane can be SP or IdP. (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 vague username or password error when login failed, you cannot tell whether the username is wrong or the password is incorrect (FIA_UAU.7).

8.1.3 Access Control

The TOE enforces an authorization policy by defining access rights that are assigned to users and roles by the **SMManagers** or the users with role administrator.

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.

The access control is based on users or groups and objects; and the security attribute object ID of an object must include the specified NE, device type, and subnet.

The access control is used to identify all the operations over objects through the NCE client if the operation rights have been assigned by the **SMManagers** or the users with role administrator (identification and authentication of operation rights)

 Copyright © Huawei Technologies Co., Ltd.

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

8.1.4 Communication Security

The TOE supports encrypted transmission between the external system and the TOE, as well as between remote users and the TOE. It implements secure data transmission mechanisms by utilizing cryptographic algorithms to establish trusted communication channels.

Communication Security between the external system and the TOE:

As a client, the TOE establishes secure communication channels with external systems (such as AAA servers, syslog servers) by employing cryptographic algorithms for key establishment, entity authentication, and data encryption.

As a server, the TOE receives connections initiated by the OSS, service orchestrators, or service applications, establishing secure channels utilizing the same cryptographic mechanisms to protect the transmitted data.

Communication Security between remote users and the TOE:

Remote users access the TOE through a web portal by initiating connections that are secured through cryptographic algorithms, ensuring the confidentiality and integrity of the data in transit.

- The security of these communication channels is fundamentally ensured by the following cryptographic functions:
- Key Establishment & Agreement: RSA and ECDH are used for secure key exchange (FCS_CKM.1/RSA, FCS_CKM.1/ECDH).
- Authentication & Digital Signatures: ECDSA and RSA are used to verify entity identities (FCS_CKM.1/ECDSA, FCS_COP.1/RSA, FCS_COP.1/ECDSA).
- Data Confidentiality: Symmetric encryption algorithms and ChaCha are applied to encrypt the payload data (FCS_COP.1/SYM, FCS_COP.1/CHACHA).
- Data Integrity: Secure Hash Algorithms are utilized to ensure data has not been altered (FCS_COP.1/SHA).
- Key Destruction: FCS_CKM.6 is applied for destruction cryptographic keys.
- Random Bit Generation: FCS_RBG.1 and FCS_RBG.3 provide the random numbers required by the key generation mechanisms (FCS_CKM.1/*).

(FTP_TRP.1, FTP_ITC.1, FCS_CKM.1/RSA, FCS_CKM.1/ECDH, FCS_CKM.1/ECDSA, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/CHACHA, FCS_COP.1/ECDSA, FCS_CKM.6, FCS_COP.1/SYM)

8.1.5 User Session Management

The TOE provides user session management including the following functions:

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

 Copyright © Huawei Technologies Co., Ltd.

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 for local and remote 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. IP address-based access control, when the IP address of the user is not within the IP policy range, the user cannot log in to the TOE.
   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. Locked and disabled status, which means the user cannot log in to the TOE in the locker or disabled status.
   e. Password Expiration Status, If the user's password has expired, the user must change the password before logging in successfully.

   (FMT_SMF.1 and FTA_TSE.1)

8.1.6 Auditing

The TOE can generate audit logs for security-relevant events as described in FAU_GEN.1. The audit log 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 NCE client by user admin and users attached to SMManagers, users with log query rights. Any user cannot delete and modify the audit logs.

Conditions for dumping logs: The number of logs in the database occupies over 1 million, the size of the logs in the database occupies over 80% of the capacity, or the number of days for storing the logs exceeds 90 days. To ensure sufficient database space, the TOE 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 TOE 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 occupy over the maximum number of logs stored in the database will be dumped.

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

 Copyright © Huawei Technologies Co., Ltd.

The TOE provides the Syslog log forwarding function, which allows audit logs to be forwarded to an external Syslog log server.

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.1, FAU_STG.2, FAU_STG.4)

Application Note:

In TOE, we use audit logs, which are called audit records in the CC standard, and the verb used to record audit logs is record. In our documentation, audit log and audit record mean the same thing.

8.1.7 Security Management Functions

The TOE provides security management if necessary. Only users assigned with roles as defined in FMT_SMR.1 or with explicitly assigned security functions 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 hashed with PBKDF2 and stored in the database.(FCS_COP.1/PBKDF2)
    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. TOE security policy, which is prior to the security attributes of individual users
    a. 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 the Same as 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. Users with role administrator also can be locked (by locking IP). 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 Administrator role in O&M plane and Management Plane.

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

8.1.8 Cryptographic Functions

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

 Copyright © Huawei Technologies Co., Ltd.

1. The TOE supports symmetric encryption and decryption using the AES-256 in GCM mode algorithm to protect sensitive data. (FCS_COP.1/SYM).
2. The TOE shall release the cryptographic key memory by overwriting the byte or char array with 0 in java and python or overwriting with 0x00 in C when the Python script invokes the C implementation to do encryption if the key is no longer used (FCS_CKM.6).
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 (HMACSHA2) algorithm from root key materials. The master key is generated with a 64-byte random number obtained from the Linux'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/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 Linux's deterministic random number generator (FCS_COP.1/PBKDF2).
5. The TOE supports controlled access to internal copies of cryptographic keys. Read and write access to these internal key copies is performed in accordance with a specified method where the keys are encrypted using an encryption key defined by the user. This ensures that cryptographic key material can only be accessed in a protected manner (FCS_CKM.3).
6. TOE provides comprehensive cryptographic functions to establish and maintain secure HTTPS communications. These cryptographic mechanisms ensure confidentiality, integrity, and authentication for network data transmission through the combination of AES for symmetric data encryption (confidentiality), ECDSA for digital signature (authentication), ECDH for key exchange, and SHA for hash functions, meeting modern HTTPS security requirements. (FCS_CKM.1/RSA, FCS_CKM.1/ECDH, FCS_CKM.1/ECDSA, FCS_COP.1/RSA, FCS_COP.1/SHA, FCS_COP.1/CHACHA, FCS_COP.1/ ECDSA, FCS_COP.1/SYM)
7. FCS_RBG.1 and FCS_RBG.3 provides the random number required by FCS_CKM.1/*.

 Copyright © Huawei Technologies Co., Ltd.

9 Abbreviations, Terminology and References

9.1 Abbreviations

Name	Explanation
CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
NBI	Northbound Interface
NE	Network Element
OSS	Operations Support System
AAA	Authentication Authorization Accounting
NTP	Network Time Protocol
BSS	Business Support System
SBI	Southbound Interface
SOP	Standard Operation Procedure
SDN	Software-defined Networking
CAS	Central Authentication Service
SSO	Single Sign-on
CMP	Certificate Management Protocol
SAML	Security Assertion Markup Language

 Copyright © Huawei Technologies Co., Ltd.

Name	Explanation
SP	Service Provider
IdP	Identity Provider
O&M	Operations and maintenance
E2E	End to End
WDM	Wavelength Division Multiplexer
OTN	Optical Transport Network
SDH	Synchronous Digital Hierarchy
OSN	NE40/PTN/Routes
NE40	Network Engine 40
PTN	Packet Transport Network
ONT	Optical Network Terminal
AP	Access Point

9.2 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
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.
O&M data	Data used for system operation and maintenance.

 Copyright © Huawei Technologies Co., Ltd.

9.3 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