CC HUAWEI iMaster NCE-T V100R021C10 - Security Target

Issue **1.5**

Date **2023-01-10**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

About This Document

Change History

Version	Date	Change Description	Author
V1.0	2022-6-29	Initial Draft	YANG Shihuan, DING Sheng
V1.1	2022-9-8	Address Review Comment	YANG Shihuan, DING Sheng
V1.2	2022-9-13	Address Review Comment	ZHANG Zixuan,WANG Yanbing, DING Sheng
V1.3	2022-12-12	Address Review Comment	ZHANG Zixuan,WANG Yanbing, DING Sheng
V1.4	2022-12-30	Address Review Comment	YANG Shihuan
V1.5	2023-01-10	Address Review Comment	YANG Shihuan

Contents

1 Introduction

This Security Target is for the evaluation of HUAWEI iMaster NCE.

1.1 ST Reference

Title: CC HUAWEI iMaster NCE-T V100R021C10 -Security Target

Version: 1.5

Author: Huawei Technologies Co., Ltd.

Publication date: 2023-01-10

1.2 TOE Reference

TOE name: HUAWEI iMaster NCE-T

TOE version: V100R021C10SPC202

TOE Developer: Huawei Technologies Co., Ltd.

TOE release date: 2023-01-10

1.3 TOE Overview

iMaster NCE is an innovative network cloud engine developed by Huawei. Positioned as the brain of future cloud-based networks, NCE integrates functions such as network management, service control, and network analysis. It is the core enablement system for network resource pooling, network connection automation and self-optimization, and O&M automation.

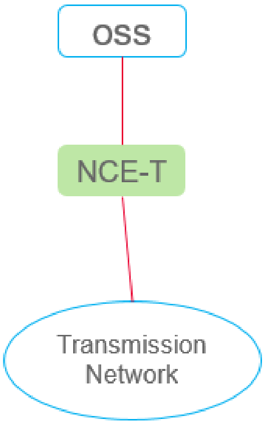
NCE is located at the management and control layer of the cloud-based network:

- NCE manages and controls transport(NCE-T) devices on lower-layer networks, supports unified management and control of SDN and legacy networks, and supports automation of single-domain, multi-domain, and cross-layer services.

  NCE can also connect to a third-party management and control system to implement cross-vendor service orchestration and automation.

- NCE also opens capabilities to support interconnection and integration with upper-layer OSSs, service orchestrators and service applications for quick customization of the application layer.

Figure 1-1 NCE deployment scenarios



As show in Figure 1-1, NCE-T is deployed in the on-premises mode where all the nodes are in the same physical environment.

The goal of NCE is to build an intent-driven network (IDN) that is first automated, then self-adaptive, and finally autonomous.

- Automated: Network deployment and maintenance are automated throughout the network lifecycle.
- Self-adaptive: Service policies are automatically generated based on big data using the real-time analyzer to implement proactive maintenance and closed-loop optimization.
- Autonomous: Artificial intelligence and machine learning are used to build an intelligent network that can automatically generate dynamic policies.

The core and base of NCE is the CloudSOP platform.

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

1.3.1 TOE Usage and Major Security Features

iMaster NCE is a unified platform that manages, controls, and maintains cloud-based SDN networks. NCE can be used in carrier, enterprise, and residential service scenarios. 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 NCE that are subject to evaluation are:

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

1.3.2 TOE Type

The TOE is a software system for cloud network management. The TOE is located at the management and control layer of the cloud-based network. It can manage and control ubiquitous network devices, including transport. It provides open interfaces to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service applications. Various apps can be developed and customized to accelerate service innovation and achieve e-commerce-style operations.

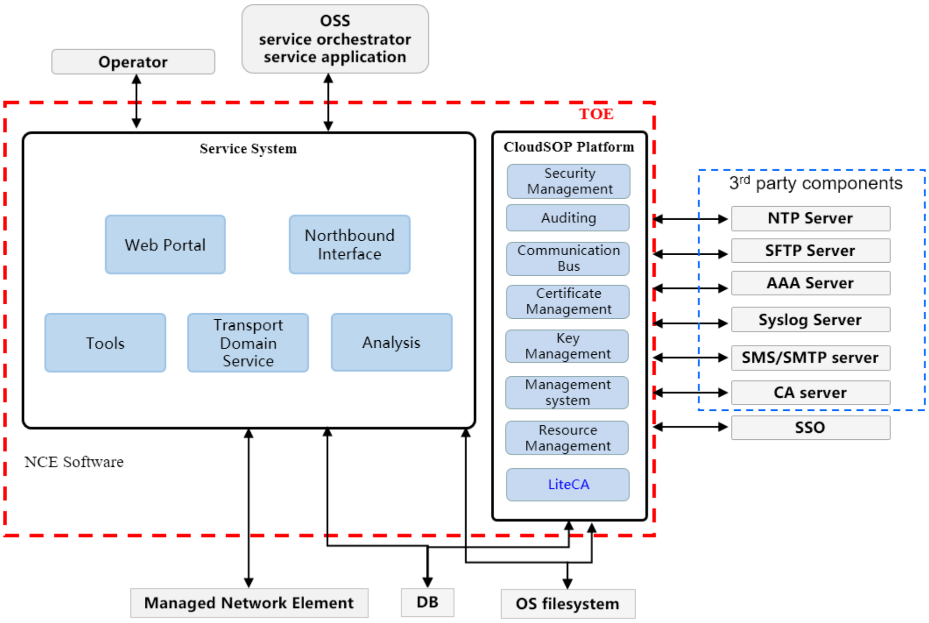
NCE is a cloud-based system that uses a service-oriented software architecture. It is deployed on a virtualized platform and can be scaled flexibly.

Based on the cloud platform, NCE implements three logical modules (network management, network control, and network analysis) and various scenario-oriented applications as services and components. This allows customers to deploy NCE in a flexible and modular manner to meet their specific requirements.

The NCE software architecture is shown in Figure 1-2. In the northbound direction, it provides Web portals and northbound interfaces for O&M personnel, OSS, service orchestrator and service application. In the southbound direction, it provides configuration and management capabilities for Huawei network devices and provides third-party driver management to manage and access third-party network adaptation drivers and third-party controllers outside the trusted zone. The system also interconnects with external NTP servers, SFTP servers, AAA authentication servers, Syslog servers, CA servers and SMS/SMTP servers.

The TOE is a class A [PP] network device management class.

Figure 1-2 TOE overview



1.3.3 Non-TOE Hardware and Software

NCE can be deployed in on-premises or private cloud mode. In On-premises mode, Huawei engineers install the hardware, virtualization environment, OS, database, and NCE software in an E2E manner. In private cloud mode (OS+product), after customers configure the virtualization environment, Huawei engineers create VMs and install OSs, databases and NCE software. Only the on premises mode is in scope of this evaluation.

NCE has specific requirements on the hardware, software and client to ensure the stable running of the system.

Hardware Configurations for On-Premises Deployment:

In on-premises scenarios, the delivered server has been configured according to the NCE requirements based on the network type, functional unit, and network scale.

For detail, see NCE Server Hardware Specifications.

For carrier users, log in to https://support.huawei.com/carrier, search NCE Server Hardware Specifications.

Configuration for the NCE Server Software:

Table 1-1 Server configuration requirements

Item	Type	Version	Remarks
Delivered software	OS	EulerOS V2.9	Used on the TaiShan server in the on-premises scenario.

configurations	Database	GaussDB T V3(Gauss100 OLTP 1.1.0)	
		Druid 0.17.0	NCE Analyzer
Compatible software configurations	Virtualization software	FushionSphere OpenStack 6.5.1 FusionSphere OpenStack 8.0.0 FusionSphere OpenStack 6.5.1	Used in the private cloud scenario.

Configuration for the NCE Client:

Table 1-2 Client configuration requirements

Type	Requirements
PC	Minimum configuration: • CPU: 2 cores, 2.6 GHz • Memory: 4 GB • Hard disk: 8 GB Recommended configuration: • CPU: 4 cores, 3.1 GHz • Memory: 8 GB • Hard disk: 8 GB
Cloud Desktop	Minimum configuration: • CPU: 4 cores, 2.6 GHz • Memory: 4 GB • Hard disk: 8 GB Recommended configuration: • CPU: 6 cores, 3.1 GHz • Memory: 8 GB • Hard disk: 8 GB
OS	• Windows 10 (32-bit or 64-bit)
Web browser	• Google Chrome 73 or later (32-bit or 64-bit, excluding 77, 78, 79, and 80) • Firefox 65 or later (32-bit or 64-bit) • Microsoft Edge 89 or later (64-bit)

Resolution	1366 x 768 px or higher; recommended resolution: 1920 x 1080 px NOTE ● Zoom ratio of the browser: 100% is recommended and 80% to 200% is compatible. ● If the resolution is within the compatibility scope of the browser, functions are available but the layout may not be user-friendly. If the resolution is not within the compatibility scope of the browser, both the functions and layout are affected.

Except the server, OS and DB as described above, the environment for TOE also comprises the following components:

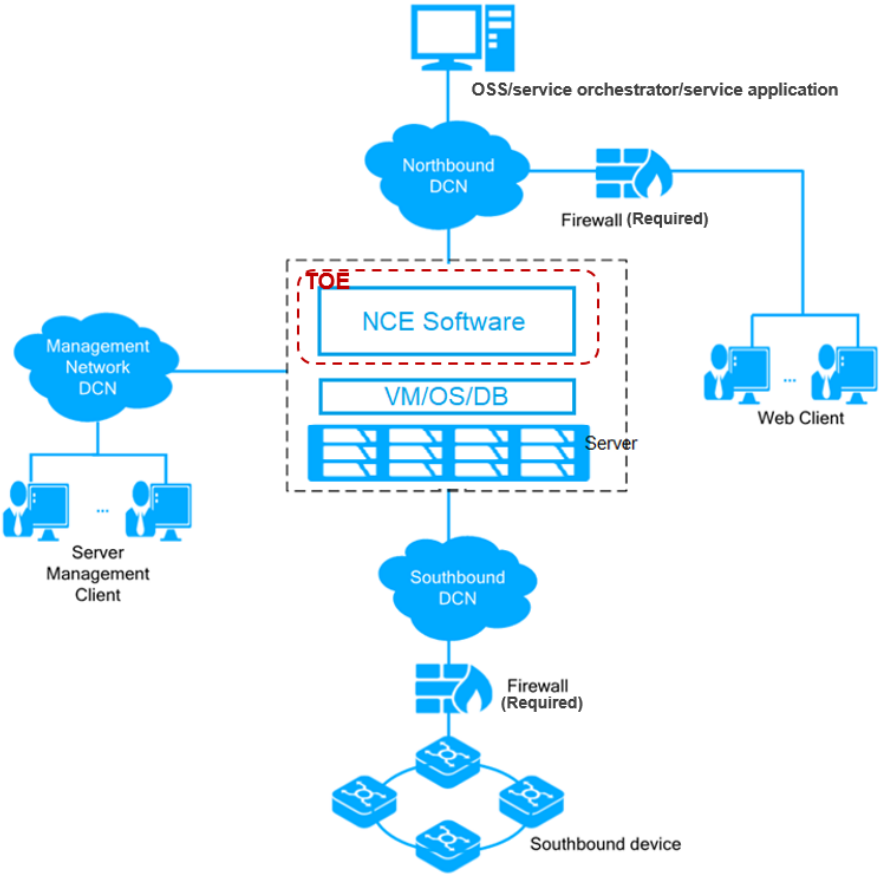
Table 1-3 Environment components

Component	Required/Optional	Usage/Purpose Description for TOE Performance
Firewall	Required	Firewall used by customers to ensure communication security between different communication planes.
Network Elements (NEs)	Required	NEs that are managed by the TOE and support different communication protocols with the TOE.
Web portal, OSSs, service orchestrators and service applications	Required	The web portal connects to the TOE using HTTPS. And the OSSs, service orchestrators and service applications that connect to the TOE through external interfaces including SNMPv3, CORBA, SFTP, Transaction Language 1(TL1), Extensible Markup Language (XML), and some customized RESTful interfaces.
AAA server	Optional	The external AAA server used to authenticate users. The TOE can correctly leverage the services provided by this AAA server to authenticate administrators. The security mechanisms for remote LDAP/RADIUS authentication depend on the third-party AAA server. Security mechanisms, such as anti-brute force cracking, password complexity check, and anti-DoS attack, must be enabled on the third-party server. Especially the communication channel between TOE and RADIUS server should be protected.
Syslog server	Optional	Syslog server used to transmit syslog messages.
SFTP server	Optional	SFTP server used to upload performance files and back up NE data.
SMS/SMTP server	Optional	NCE sends notifications by emails or messages.
CA server	Optional	CA server can apply for a certificate, update the

Component	Required/Optional	Usage/Purpose Description for TOE Performance
		certificate, and publish the CRL certificate revocation list (CRL) file.
NTP server	Required	NTP server is used to sync the time of the NCE server.
EasySuite	Required	EasySuite used to install and deploy NCE. The tool, which is managed by a single user, encrypts sensitive information such as passwords for storage and protection, protects the software package against tampering through digital signature verification, and ensures the security of the tool using the EasySuite security mechanism. NCE is installed using EasySuite and security hardening is performed on EulerOS by default, including OS account and password security, system service/component minimization, file/directory permission minimization, authentication and authorization, kernel parameter security, and system log audit. For details, see the AGD document. EulerOS itself is not included in the TOE.
FusionInsight	Required	Huawei FusionInsight MRS is a distributed data processing system that provides large-capacity data storage, query, and analysis capabilities.

Figure 1-3 shows the physical environment of NCE, which is the typical environment.

Figure 1-3 TOE physical environment



1.4 TOE Description

1.4.1 TOE Definition Scope

This section will define the scope of the iMaster NCE to be evaluated. NCE can be deployed in on-premises or private cloud mode. Only on-premises mode is certified. For details about the configuration specifications for the two modes, see 1.3.3 Non-TOE Hardware and Software.

1.4.1.1 Physical Scope

The TOE is a software only and the TOE is to be installed on a specified non-TOE hardware server. The servers, OSs, and databases make up the TOE environment to meet the security requirements.

Users can log in to the HUAWEI support website to download 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).

NCE software package consists of binary compressed files. The following software packages and documents are required and are part of the TOE. NCE supports four deployment scenarios. The following table lists the software packages corresponding to NCE-T deployment scenario.

Table 1-4 TOE software list

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
NCE Management Plane Service Package	iMasterNCE_V100R021C10SPC202_OMP_linux-aarch64.zip	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_OMP_linux-aarch64.zip.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_OMP_linux-aarch64.zip.crl	V100R021C10SPC202	√
NCE Management Plane Service Package	iMasterNCE_V100R021C10SPC202_BKSigntool_linux-aarch64_pkg.tar	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_BKSigntool_linux-aarch64_pkg.tar.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_BKSigntool_linux-aarch64_pkg.tar.crl	V100R021C10SPC202	√
NCE O&M Plane Service Package	iMasterNCE_V100R021C10SPC202_CloudSOPCloudService_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_CloudSOPCloudService_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	**Deliverable Name**	**Version**	**Deployment Scenario**
			NCE-T
	iMasterNCE_V100R021C10SPC202_CloudSOPCloudService_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Common Service Package	iMasterNCE_V100R021C10SPC202_CommonService_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_CommonService_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_CommonService_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Common Service Package	iMasterNCE_V100R021C10SPC202_ProductSolution_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_ProductSolution_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_ProductSolution_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management Service Package	iMasterNCE_V100R021C10SPC202_NMSBase_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSBase_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCE_V100R021C10SPC202_NMSBase_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management Service Package	iMasterNCE_V100R021C10SPC202_NMSPMS_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSPMS_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSPMS_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_NMSIPE2E_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSIPE2E_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSIPE2E_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_NMSNBI_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSNBI_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCE_V100R021C10SPC202_NMSNBI_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_NMSiMap_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSiMap_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSiMap_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_NMSDC_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSDC_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSDC_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_NMSTrans_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NMSTrans_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCE_V100R021C10SPC202_NMSTrans_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Tool Service Package	iMasterNCE_V100R021C10SPC202_UniCollect_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_UniCollect_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_UniCollect_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Tool Service Package	iMasterNCE_V100R021C10SPC202_NetworkDataIngestion_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NetworkDataIngestion_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_NetworkDataIngestion_linux-aarch64.7z.crl	V100R021C10SPC202	√
Analyze Service Package	iMasterNCE_V100R021C10SPC202_Analyzer_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_Analyzer_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCE_V100R021C10SPC202_Analyzer_linux-aarch64.7z.crl	V100R021C10SPC202	√
Analyze Service Package	iMasterNCE_V100R021C10SPC202_AnalyzerCommon_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_AnalyzerCommon_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_AnalyzerCommon_linux-aarch64.7z.crl	V100R021C10SPC202	√
Analyze Service Package	iMasterNCE_V100R021C10SPC202_AnalyzerODAE_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_AnalyzerODAE_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_AnalyzerODAE_linux-aarch64.7z.crl	V100R021C10SPC202	√
Analyze Service Package	iMasterNCEServerInstall_V100R021C10SPC202_BigDataAnalyzer_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCEServerInstall_V100R021C10SPC202_BigDataAnalyzer_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCEServerInstall_V100R021C10SPC202_BigDataAnalyzer_linux-aarch64.7z.crl	V100R021C10SPC202	√
Analyze Service Package	iMasterNCE_V100R021C10SPC202_LegacyCollector_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_LegacyCollector_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_LegacyCollector_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Management	iMasterNCE_V100R021C10SPC202_ExtNBIRCA_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_ExtNBIRCA_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_ExtNBIRCA_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE T Service Package	iMasterNCE_V100R021C10SPC202_ACTrans_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_ACTrans_linux-aarch64.7z.cms	V100R021C10SPC202	√

Deliverable Type	Deliverable Name	Version	Deployment Scenario
			NCE-T
	iMasterNCE_V100R021C10SPC202_ACTrans_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE T Service Package	iMasterNCE_V100R021C10SPC202510_NetStarOM_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202510_NetStarOM_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202510_NetStarOM_linux-aarch64.7z.crl	V100R021C10SPC202	√
NCE Service Package	iMasterNCE_V100R021C10SPC202_LiteCA_linux-aarch64.7z	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_LiteCA_linux-aarch64.7z.cms	V100R021C10SPC202	√
	iMasterNCE_V100R021C10SPC202_LiteCA_linux-aarch64.7z.crl	V100R021C10SPC202	√

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

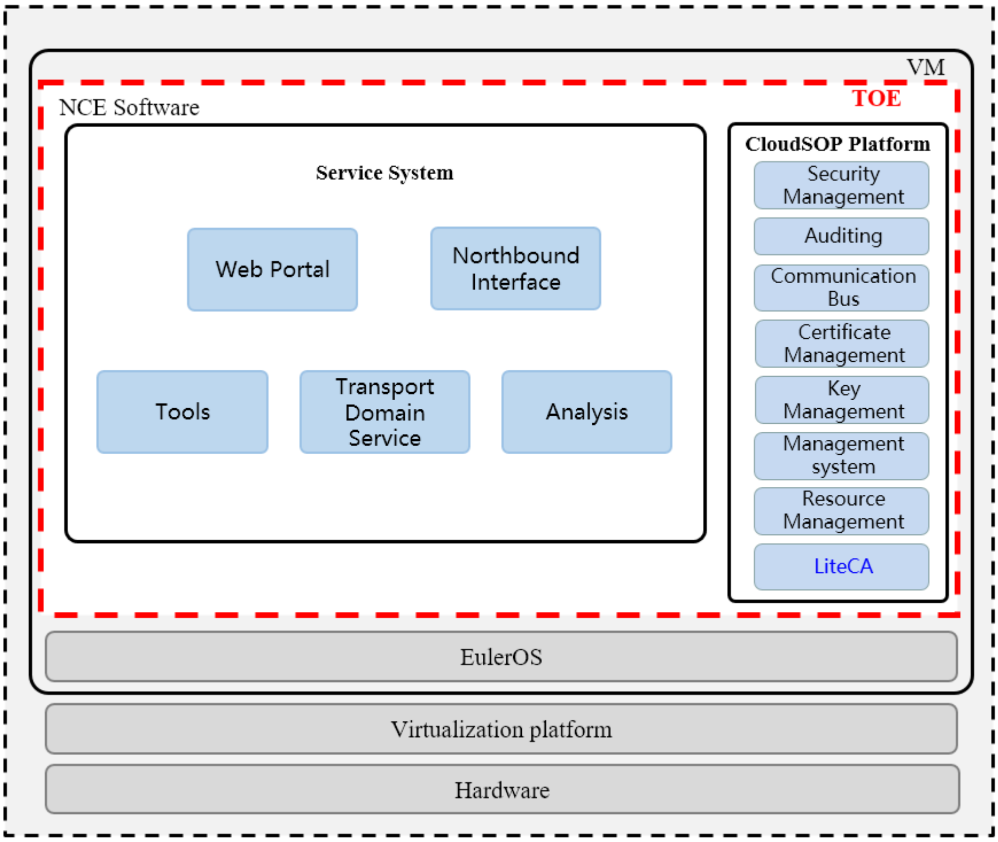
Table 1-5 TOE guidance list

Name	**Version and date**	**Deployment Scenario**
iMaster NCE-T V100R021C10 Product Documentation	02-C, 2022-09-30	NCE-T
iMaster NCE V100R021C10 Product Documentation (Project Deployment & System Maintenance, Arm)	04-C, 2022-09-30	ALL
CC HUAWEI iMaster NCE V100R021C10 -Installation Guide	V1.2, 2023-01-11	ALL
CC HUAWEI iMaster NCE V100R021C10 -Security Management Guide	V1.2, 2023-01-09	ALL

1.4.1.2 Logical Scope

NCE integrates functions such as network management, service control, and network analysis. The TOE boundary from a logical point of view is represented by the elements that are displayed in the red box in the figure below.

Figure 1-4 TOE logical scope



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

User Management

On the management plane, 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 including **Administrators**, **SMManagers**, **NBI User Group**, **Maintenance Group**, **Operator Group** and **Guests**. 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 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 through the TOE client.

Communication Security

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

User Session Management

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

Auditing

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

Logs record routine maintenance events of the TOE. For security purposes, the TOE provides security logs and operation logs.

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

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

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

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

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

Security Management Functions

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

Cryptographic Function

Cryptographic functions are dependencies required by security features. The TOE supports cryptographic algorithms as described in section 5.2.7 Cryptographic Support.

2 Conformance Claims

2.1 CC conformance claim

This ST is CC Part 2 conformant [CC] and CC Part 3 conformant [CC]. The version of [CC] is 3.1 Revision 5.

This ST is EAL4+ALC_FLR.2 as defined in [CC] Part 3.

The methodology to be used for evaluation is [CEM] 3.1 R5.

2.2 PP conformance claim

This ST is claims strict conformance to [PP] "Common Criteria Protection Profile for Network Device Management (NDhPP) v1.0 2021-4-23."

The TOE type is a network management system, which is consistent with the Class A type of TOE defined in the [PP].

2.3 Overview of differences between the PP and the ST

Security Functional Requirements

The Security Target enhances security functional requirements to support additional Cryptographic Key Generation and Cryptographic operation (FCS_CKM.1/FCS_COP.1).

The additions do not contradict any of the threats, assumptions, organizational policies, objectives or SFRs stated in the [PP] that covers the advanced security methods in operational use phase.

3 Security Problem Definition

3.1 Assumptions

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

It is assumed that the software platform of the server that the TOE is running on (as listed in section 1.4.1 TOE Definition Scope) is protected against unauthorized physical access.

It is assumed that the database is protected against data file damage.

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

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 will behave correctly and will not perform any harmful operation on the TOE.

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

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

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

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

A.FusionInsight It is assumed FusionInsight are considered trusted and will not attack the TOE and the communication to FusionInsight is under protection.

3.2 Threats

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

3.2.1 Assets and Agents

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

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

3.2.2 Threats Addressed by the TOE

3.2.2.1 T.UnauthenticatedAccess

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

3.2.2.2 T.UnauthorizedAccess

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

3.2.2.3 T.Eavesdrop

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

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

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

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

4.2 Security Objectives for the Operational Environment

1. **OE.NetworkElements** The operational environment ensures that the trusted NEs support the TLS /SNMPv3/SSHv2/SFTP/HTTPS connection with the TOE and private interface defined by Huawei.
2. **OE.Physical** The TOE is protected against unauthorized physical access.
3. **OE.NetworkSegregation** The operational environment protects the network where the TOE hosts are installed by separating it from the application (or public) network. A firewall is installed between the TOE server and untrusted domain to filter unused communication ports.
4. **OE.Database** The operational environment protects the database against unauthorized physical access and data file damage.
5. **OE.AdministratorBehaviour** The super user **admin**, the users who belong to the **SMManagers** and **Administrators** groups and the users of the underlying operating system will behave correctly and will not perform any harmful operation on the TOE.

6. **OE.NTP** The operational environment provides an accurate time source, in order to ensure normal operations on the TOE server.
7. **OE.TrustedPlatform** The operation environment provides a trusted platform like OS, DB, hardware, virtual machine.
8. **OE.Components** The 3rd party components are considered trusted and will not attack the TOE. The administrator shall ensure the communication between the TOE and the NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, and CA server is secured when these servers are used.
9. **OE.FusionInsight** FusionInsight builds a reliable, secure, and easy-to-use operation and maintenance (O&M) platform and provides storage and analysis capabilities for massive data, helping address enterprise data storage and processing demands.

4.3 Security Objectives Rationale

4.3.1 Coverage

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

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

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

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

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

4.3.2 Sufficiency

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

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

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

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

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

Assumption	Rationale for Security Objectives
A.FusionInsight	The assumption that FusionInsight are considered trusted and will not attack the TOE and the communication to FusionInsight is under protection is addressed by OE. FusionInsight.

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

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

5 Security Requirements for the TOE

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (Underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicized and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

5.2 Security Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

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

a Start-up and shutdown of the audit functions;
b All auditable events for the [***not specified***] level of audit; and
c [The following auditable events:

1. User activity

(a) login, logout events

2. User management

(a) add, delete, modify users

(b) user password change

3. [assignment:

i. User group (role) management

a) Creating, deleting, and modifying user groups

b) Granting access rights to user groups

c) Granting access rights to user accounts

ii. **Security policy management**

a) **Modifying password policies**

b) **Modifying user account policies**

iii. **User session management**

Kicking out individual user sessions

iv. **ACL management**

a) **Creating, deleting, and modifying ACLs**

b) **Specifying ACLs for individual user account.**

v. **Region, operation set and device set management**

vi. **Audit log management**

vii. **Certificate management**

viii. **NE management].s**

FAU_GEN.1.2

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

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

5.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1

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

Application Note: the audit records include security logs, operation logs, system logs.

FAU_SAR.1.2

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

Application Note:

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

Log Type	Permission
Security logs generated by all users	**Query Security Log**
System logs	**Query System Log**

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

5.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1

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

5.2.1.5 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**].

5.2.1.6 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1

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

FAU_STG.1.2

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

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

FAU_STG.3.1

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

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.2 Completing Access Control

FDP_ACC.2.1

The TSF shall enforce the [**Access Control SFP**] on [**Subject: users; Objects: commands provided by TOE**] 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.

5.2.2.2 FDP_ACF.1 Security Attribute-Based Access Control

FDP_ACF.1.1

The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [

1. **Subject security attributes:**
   Users and their following security attributes
   - ~~**User identity**~~
   - ~~**User level**~~
   - **(User ID**
   - **User type**
   - **User role assignment)**
2. **Objects security attributes:**
   Commands and their security attributes
   - ~~**Command level**~~
   - **(Device ID)**

   ]

Application Note: For TOE, user ID is the user identity, user type and role assignment is corresponding to user level, and the device ID is the object security attribute.

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. **(An operation set contains many operation rights that are assigned to specific user roles.)**
2. **Only authorized users are permitted access to commands.**
3. **Users can be configured with different user levels to control the TOE access permission.**
4. **There are [~~number of user access levels~~] different user access levels and command levels (based on user role assignment).**
5. **A user can access a command if the command's access level is lower or equal to the user's access level.**
6. **The command level is stored by the TOE and [can] be modified by [SMManagers]**

Application Note: user will be assigned to specific user roles and acquire different user access levels and operation rights.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ~~none~~ (**explicitly assigned security functions**).

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

FDP_ACF.1.4

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

5.2.2.3 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1

The TSF shall ~~enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to~~ **[*transmit and receive*]** ~~user data~~ (certificate to/from CA server) in a manner protected from **[*modification, insertion*]** errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of ~~user data~~ (certificate to/from CA server), whether **[*modification, insertion*]** has occurred.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1

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

5.2.3.2 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.

5.2.3.3 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1

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

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

1. **When local authentication is enabled, user authentication is implemented by TOE itself.**
2. **When LDAP authentication is enabled, user authentication is implemented by a remote LDAP server.**
3. **When RADIUS authentication is enabled, user authentication is implemented by a remote RADIUS server.**
4. **When CAS or SAML SSO configuration is enabled, user authentication is implemented by the SSO server of the TOE, and the user can log into all trusted SSO clients of other TOE instances without being authenticated again after logging in to**

one of the trusted TOEs.]

5.2.3.4 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1

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

5.2.3.5 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.

5.2.3.6 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. **User level**
3. **User password**
4. **The inactivity time after which an account is automatically logged out.**
5. **Status of the account (locked/unlocked)**
6. **Number of failed authentication attempts within a certain period of time and timestamp of last successful login**
7. **[assignment:**

Username

User type

Mobile number, optional

Email address, optional

Welcome message, optional

Login time policy

Client IP address policy

User role assignment

Maximum online sessions, optional

Account validity period (days), optional

Select the policy (Disable user, Delete user, Unlimited) if no login within a period (configurable days), optional

Compulsory password renewal (Password validity period (days), In advance warning before password expires (days), Minimum password usage period (days)), optional]].]

5.2.3.7 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**].

User roles	O&M Plane (by default)	Web Management (by default)
Admin (super user admin)	10 minutes	10 minutes
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	
Guest 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	
Analyzer User Group only on the O&M plane	30 minutes	
HOFS Group only on the O&M plane	30 minutes	

5.2.3.8 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(8)**
2. **Min. system administrator password length(8)**
3. **Max. password length(32)**
4. **Configurable number of latest passwords that cannot be reused**
5. **Password repetition not allowed within configurable number of months**
6. **Min. password usage period (days) (10)**
7. **Password validity period (days)**
8. **Force logout upon password reset**
9. **Min. characters different between new and old passwords (3)**
10. **Min. number of letters**
11. **Min. number of uppercase letters**
12. **Min. number of lowercase letters**

13. **Min. number of digits**
14. **Min. number of special characters**
15. **Password that cannot contain spaces**
16. **Password that cannot contain its username in reverse order**
17. **Password that cannot be an increasing, decreasing, or interval sequence of digits or letters**
18. **Policy about max. consecutive characters used in both username and password**
19. **Policy that the password cannot contain repeated character sequences**
20. **Max. times a character can consecutively occur(2)**
21. **Password that cannot contain user's mobile number or email address**
22. **Password that cannot contain words in the uploaded password dictionary file or hacker language dictionary configured in the backend file]**

Application Note: The defined quality metrics are configurable by the administrator.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

1. **Management of user accounts and user attributes, including user credentials**
2. **Management of authentication failure policy**
3. **Configuration of network addresses for services used by the TOE**
4. **Enabling/disabling trusted channels for remote access to the TOE’s management interfaces**
5. **Management of the TOE’s time**
6. **[Audit log management**
7. **Certificate management**
8. **NE management**
9. **Client IP Address Policies (ACL)**
10. **Login time policy**
11. **Configuration of the time interval of user inactivity for terminating an interactive session**
12. **Command group management**

].

5.2.4.2 FMT_SMR.1 Security Roles

FMT_SMR.1.1

The TSF shall maintain the roles: [

1. **Administrators both on the management and O&M plane**
2. **SMManagers both on the management and O&M plane**

3. **Monitors only on the management plane**
4. **Operators only on the management plane**
5. **NBI User Group only on the O&M plane**
6. **Guest only on the O&M plane**
7. **Maintenance Group only on the O&M plane**
8. **Operator Group only on the O&M plane**
9. **Analyzer User Group only on the O&M plane**
10. **HOFS 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.

5.2.4.3 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1

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

Application Note:

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

Role Name	Security Functions
Administrators	**Certificate management** **Command group management** **NE management**
SMManagers	**Authentication mode configuration** **User management** **Role management** **Account policy** **Password policy** **Audit log management** **Client IP Address Policies (ACL)** **Login time policy** **Configuration of the time interval of user inactivity for terminating an interactive session**
Monitors	The user group has permission to monitor non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, server tracing, NAT configuration, information collection, trouble shooting, emergency system, cloud service management,infrastructure, commissioning wizard, etc.

Role Name	Security Functions
Operators	The user group has permission to perform non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, trace server product tool, configure NAT tool, information collection, trouble shooting, emergency system, cloud service management,infrastructure, commissioning wizard, etc.
NBI User Group	**Configuration of trusted channels for connecting to the external entities**
Guest	**Granted by SMManagers**
Maintenance Group	**NE Management** **Configuration of trusted channels for connecting to the external entities**
Operator Group	**NE Management** **Command group management** **Configuration of trusted channels for connecting to the external entities**
user-defined User Group	**Granted by SMManagers**
HOFS Group	Has the permission for HOFS file system
Analyzer User Group	Has the permission for analysis module

5.2.4.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1

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

5.2.4.5 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1

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

5.2.4.6 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1

The TSF shall enforce the [**NCE 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.

5.2.5 TOE Access (FTA)

5.2.5.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on

1. **User authentication failure**
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. **System login mode]**

Application Note:

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

5.2.5.2 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**].

5.2.5.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

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

5.2.5.4 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.

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 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 **[*initial user authentication and remote management*].**

5.2.6.2 FTP_ITC.1/External System Inter-TSF Trusted Channel

FTP_ITC.1.1

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

FTP_ITC.1.2

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

FTP_ITC.1.3

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

5.2.6.3 FTP_ITC.1/NE Inter-TSF Trusted Channel

FTP_ITC.1.1

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

FTP_ITC.1.2

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

FTP_ITC.1.3

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

5.2.7 Cryptographic Support (FCS)

5.2.7.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1/1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[PBKDF2]** and specified cryptographic key sizes **[128 bits]** that meet the following: **[RFC8018 chapter 5.2]**

FCS_CKM.1.1/2

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[RSA]** and specified cryptographic key sizes **[2048 bits, 3072 bits, 4096 bits, 8192 bits]** that meet the following: **[RFC 8017]**

FCS_CKM.1.1/3

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: **[RFC6979]**

5.2.7.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwriting with 0 in java and python or overwriting with 0xcc in C when the Python script invokes the C implementation to do encryption]** that meets the following: **[none]**.

5.2.7.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/1

The TSF shall perform **[symmetric de- and encryption]** in accordance with a specified cryptographic algorithm **[AES GCM Mode]** and cryptographic key sizes **[128 bits]** that meet the following: **[FIPS 197 chapter 5, NIST SP 800-38A chapter 6.2]**

FCS_COP.1.1/2

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

FCS_COP.1.1/3

The TSF shall perform **[digital signature operation]** in accordance with a specified cryptographic algorithm **[RSASSA-PSS, RSASSA-PKCS1-v1_5]** and cryptographic key sizes **[2048bits, 3072bits, 4096bits, 8192bits]** that meet the following: **[RFC8017].**

FCS_COP.1.1/4

The TSF shall perform **[digital signature operation]** in accordance with a specified cryptographic algorithm **[ECDSA]** and cryptographic key sizes **[256bits, 384bits, 521bits]** that meet the following: **[RFC6979].**

5.2.8 Protection of The TSF (FPT)

5.2.8.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1

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

5.3 Security Functional Requirements Rationale

5.3.1 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.3	O.Audit
FDP_ACC.2	O.Authorization
FDP_ACF.1	O.Authorization
FPT_ITT.1	O.Communication

Security Functional Requirements	Objectives
FDP_UIT.1	O.Communication
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
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
FMT_MSA.3	O.Authorization
FTA_TSE.1	O.Authentication
FTA_SSL.3	O.Authentication
FTA_SSL.4	O.SecurityManagement
FTA_TAH.1	O.Authentication
FTP_TRP.1	O.Communication
FTP_ITC.1/ External System	O.Communication

Security Functional Requirements	Objectives
FTP_ITC.1/NE	O.Communication
FCS_CKM.1/1	O.SecurityManagement
FCS_CKM.1/2 FCS_CKM.1/3	O.Communication
FCS_CKM.4	O.SecurityManagement
FCS_COP.1/1	O.SecurityManagement
FCS_COP.1/2	O.Authentication O.SecurityManagement
FCS_COP.1/3	O.Communication
FCS_COP.1/4	O.Communication

5.3.2 Sufficiency

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

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by (FAU_GEN.1). Audit records are supposed to include user identities (FAU_GEN.2) where applicable, which are supplied by the identification mechanism (FIA_UID.2). Audit records are stored in the database, and are filtered to read and search with conditions, and restricted audit review requires authorized users (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3). Management functionality for the audit mechanism is spelled out in (FMT_SMF.1). The audit record is stored in the database, and exported into a file if the size of the audit record occupies over the configured maximum size (FAU_STG.1, FAU_STG.3).
O.Communication	Communication security is implemented by data integrity protection (FDP_UIT.1) between TOE and the CA server, trusted channels (FTP_ITC.1/External System, FTP_ITC.1/NE) between TOE and external servers, and (FTP_TRP.1) between TOE and the web clients. NE performance data bulk collection and backup and software update are implemented through the secure channel. NCE communicates with NEs through secure channels to manage and control NE devices, including Huawei transport access devices, data communication devices, SDN controllers, and third-party network devices. (FTP_TRP.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

Security objectives	Rationale
	communication is provided in (FMT_SMF.1). Services are accessed through the TLS security protocol. (FPT_ITT.1) The TOE integrates a private CA called LiteCA for issuing TLS certificates to internal services or NEs (FCS_COP.1.1/3, FCS_COP.1.1/4). The certificate key type can be either RSA (FCS_CKM.1.1/2) or ECDSA (FCS_CKM.1.1/3).
O.Authentication	User authentication (including re-authentication) is implemented by (FIA_UAU.2, FIA_UAU.5, FIA_UAU.6) and supported by individual user identities in (FIA_UID.2). The necessary user attributes (passwords) are spelled out in (FIA_ATD.1). The authentication mechanism supports authentication failure handling (FIA_AFL.1), restrictions as to the validity of accounts for login (FTA_TSE.1), and a password policy (FIA_SOS.1). Management functionality is provided in (FMT_SMF.1). The TOE logs off sessions when they are inactive for a configured period of time (by default 30 minutes) (FTA_SSL.3). The session establishment shall be denied based on security attributes (FTA_TSE.1). Authentication feedback information is protected by (FIA_UAU.7). TOE shall display access history of the last successful and unsuccessful logins (FTA_TAH.1). For password verification hash values of passwords are used which are generated using FCS_COP.1/PBKDF2. The authentication mechanism for NBIs and NEs to connect to NCE is also implemented by FIA_UAU.2.
O.Authorization	The requirement for access control is spelled out in (FDP_ACC.2), and the access control policies are modeled in (FDP_ACF.1) for accessing the NCE server. Unique user IDs are necessary for access control (FIA_UID.2), and user authentication (FIA_UAU.2, FIA_UAU.5). User-related attributes are spelled out in (FIA_ATD.1). Access control is based on the definition of roles as subjects and functions as objects (FMT_SMR.1). Management functionality for the definition of access control policies is provided (FMT_MSA.1, FMT_MSA.3, FMT_SMF.1). User re-authentication is implemented by (FIA_UAU.6) If a user fails to log in to the system for multiple consecutive times, the locking policy for the account and IP address is executed (FIA_AFL.1).
O.SecurityManagement	Management functionality is provided in (FMT_SMF.1/FIA_ATD.1/FIA_SOS.1/FMT_SMF.1/FMT_MOF.1 / FMT_MTD.1/FTA_SSL.4). The AES algorithm is used to encrypt sensitive information such as users' mobile numbers and email addresses. (FCS_CKM.1/1, FCS_CKM.4, FCS_COP.1/1, FCS_COP.1/2)

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

	O.Audit	O.Authorization	O.Authentication	O.Communication	O.SecurityManagement
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_STG.1	X				
FAU_STG.3	X				
FDP_ACC.2		X			
FDP_ACF.1		X			
FPT_ITT.1				X	
FDP_UIT.1				X	
FIA_UID.2	X	X	X		
FIA_UAU.2		X	X		
FIA_UAU.5		X	X		
FIA_UAU.6		X	X		
FIA_UAU.7			X		
FIA_ATD.1		X	X		X
FIA_AFL.1		X	X		
FIA_SOS.1			X		X
FMT_SMF.1	X	X	X	X	X
FMT_SMR.1		X			
FMT_MOF.1					X
FMT_MTD.1					X
FMT_MSA.1		X			
FMT_MSA.3		X			
FTA_TSE.1			X		
FTA_SSL.3			X		
FTA_SSL.4					X
FTA_TAH.1			X		
FTP_ITC.1/External System				X	

	O.Audit	O.Authorization	O.Authentication	O.Communication	O.SecurityManagement
FTP_ITC.1/NE				X	
FCS_CKM.1/AES					X
FCS_CKM.4					X
FCS_COP.1/AES					X
FCS_COP.1/PBKDF2			X		X

5.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL4 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

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

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

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Resolved by external time source. The audit time depends on the reliable time stamp. Reliable time stamp depends on external time sources
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.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
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3

Security Functional Requirement	Dependencies	Resolution
FDP_UIT.1	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	FDP_ACC.2 and FDP_IFC.1 are not applicable because there is no access control or information flow control enforced. FTP_ITC.1 and FTP_TRP.1 are not applicable because there is no confidentiality issue and no trusted path.
FIA_UID.2	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.1	None	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FTA_TSE.1	None	None
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAH.1	None	None
FTP_TRP.1	None	None

Security Functional Requirement	Dependencies	Resolution
FTP_ITC.1/ External System	None	None
FTP_ITC.1/NE	None	None
FCS_CKM.1/AES	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/AES	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	PBKDF2 is a hash algorithm with no key.
FPT_ITT.1	None	None

5.4 Security Assurance Requirements

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

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

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

5.5 Security Assurance Requirements Rationale

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

6 TOE Summary Specification

6.1 TOE Security Functionality

6.1.1 User Management

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

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

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**. The super user **admin** can complete all the functions, including security and administrative functions. During user permission maintenance period, security administrators can view and modify user, role, user group, and operation set information, and monitor user sessions and operations in real time, ensuring system security.

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

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

Role Name	Description	Scenario
Administrators	The user group has all the permissions except user management, query security log, query personal security log and view online users.	ALL
SMManagers	The user group has permission to manage users, manage licenses, query security logs, view online users, and update ACL policies.	ALL
Monitors	The user group has permission to monitor non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, server tracing, NAT configuration, information collection, trouble shooting, emergency system, cloud service management, infrastructure, commissioning wizard, etc.	ALL
Operators	The user group has permission to perform non-security operations of backup and restore, deployment, system monitoring, maintenance, system settings, alarms, the disaster recovery (DR) system, product planning, server tracing, NAT configuration, information collection, trouble shooting, emergency system, cloud service management, infrastructure, commissioning wizard, etc.	ALL

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

Role Name	Description	Scenario
Administrators	The user group has all the permissions except **User Management**, **Query Security Log**, **View Online Users**, and **Query Personal Security Log**.	NCE-T
SMManagers	The user group has the **User Management**, **License Manager**, **View Online Users**, and **Query Security Log** permissions.	NCE-T
NBI User Group	The user group has the permission to configure the northbound interfaces such as SNMP, CORBA, XML, TEXT and RESTful NBIs.	NCE-T
Guest	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,	NCE-T

Role Name	Description	Scenario
	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 NCE and NEs.	NCE-T
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.	NCE-T
Analyzer User Group	Analyzer User Group.	NCE-T
HOFS Group	Has the File Management Operation Set permission.	NCE-T

6.1.2 Authentication

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

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

The TOE shall verify that the password meets the following password policies which are configurable by the administrator: [

1. Min. password length**(8)**
2. Min. system administrator password length**(8)**
3. Max. password length**(32)**
4. Configurable number of latest passwords that cannot be reused
5. Password repetition not allowed within the configurable number of months
6. Min. password usage period (days) **(10)**
7. Password validity period (days)
8. Force logout upon password reset

9. Min. characters different between new & old passwords**(3)**
10. Min. number of letters
11. Min. number of uppercase letters
12. Min. number of lowercase letters
13. Min. number of digits
14. Min. number of special characters
15. Password that cannot contain spaces
16. Password that cannot contain its username in reverse order
17. Password that cannot be an increasing, decreasing, or interval sequence of digits or letters
18. Policy about max. consecutive characters used in both the username and password
19. Policy that the password cannot contain repeated character sequences
20. Max. times a character can consecutively occur**(2)**
21. Password that cannot contain user's mobile number or email address
22. Password that cannot contain words in the password dictionary or hacker language dictionary]

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

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

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.
If three accounts using a client IP address are locked within 10 minutes, this client IP address will be locked for 30 minutes.

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, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, 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 username or password error when login failed (FIA_UAU.7).

6.1.3 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)

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

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

(FMT_SMF.1 and FTA_TSE.1)

6.1.4 Communication Security

The TOE supports encrypted transmission between NEs and the TOE, the external system and the TOE, remote user and the TOE. It provides secure protocols, such as TLS, SNMPv3, SSHv2 and SFTP, for data transmission. The TOE integrates a private CA called LiteCA for issuing TLS certificates to internal services or NEs (FCS_COP.1.1/3, FCS_COP.1.1/4). The certificate key type can be either RSA (FCS_CKM.1.1/2) or ECDSA (FCS_CKM.1.1/3).

Communication Security between NEs and the TOE:

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

Communication Security between the external system and the TOE:

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

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

Communication Security between remote users and the TOE:

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

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

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

Communication Security inside the TOE:

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

6.1.5 User Session Management

The TOE provides user session management. The function includes 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 will generate an alarm. The session establishment will be denied based on the policy below (FTA.TSE.1).

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

2. TSF-initiated session Termination

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

3. User-initiated session termination

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

4. Users and their following security attributes:
   (a) Time segment for login, which means that the user shall log in to the TOE within a specific time segment.
   (b) ACL, addressed in the previous section.
   (c) Maximum online sessions, which indicates that the number of online sessions shall not exceed the maximum sessions, otherwise the user login requests after the maximum online sessions shall be refused by the TOE. The default is none.
   (d) Disabled status, which means the user cannot log in to the TOE in the disabled status.
5. System security policy, which is prior to the security attributes of individual users

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

6.1.6 Auditing

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

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

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

Conditions for deleting log files: The size of the log files is greater than 1024 MB (default value), the log files are stored for more than 45 days (default value), or the total number of log files exceeds 1000 (default value). To ensure sufficient disk space, the system checks log files every hour and deletes log files meeting the requirements from the hard disk.

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

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.3)

6.1.7 Security Management Function

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

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

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

6.1.8 Cryptographic Functions

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

1. The TOE supports symmetric encryption and decryption using the AES256-GCM algorithm to protect sensitive data. (FCS_COP.1/AES).
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 0xcc in C when the Python script invokes the C implementation to do encryption if the key is no longer used (FCS_CKM.4).
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 TOE's deterministic random number, the master key is encrypted and protected by the root key. The working key is generated by PBKDF2 (HMACSHA2) algorithm from master key materials, the working key is encrypted and protected by the master key, the working key is used to provide confidential and complete protection for sensitive data saved in a local PC or data transferred through insecure channels. Both the two keys can be updated manually (FCS_CKM.1).
4. The TOE supports hashing of data using PBKDF2 (SHA256) algorithm according to [RFC8018] for password hashing. The iteration number is at least 10,000 times. The salt used in PBKDF2 is a 16-byte random number obtained from the TOE's deterministic random number generator (FCS_COP.1/PBKDF2).
5. The TOE supports issuing certificates and can generate RSA, ECDSA key pairs according to the key generation algorithm described in FCS_CKM.1. Then, perform the corresponding digital signature operation according to the digital signature algorithm described in FCS_COP.1 to generate the certificate.

7 Abbreviations, Terminology and References

7.1 Abbreviations

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
OM	Operation and Maintenance
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
CA	Certificate Authority
CAS	Central Authentication Service
SSO	Single Sign-on
CMP	Certificate Management Protocol

SAML	Security Assertion Markup Language
SP	Service Provider
IdP	Identity Provider
AOC	Agile Open Container
CSP	Cloud Service Provider

7.2 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.
OM data	Data used for system operation and maintenance.

7.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2019. Version 3.1 Revision 5.

[CEM] Common Methodology for Information Technology Security Evaluation. September 2019. Version 3.1 Revision 5.

[PP] Common Criteria Protection Profile for Network Device Management (NDhPP), Version 1.0, 2021-04-23.