EUCC Certification Report

CERTIFICATION REPORT INFORMATION	
Certification Report Reference	**FCS506_05 EUCC HUAWEI iMaster NCE Certification Report v1.0**
Project (TOE) Identification	TOE Name: HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100) TOE version: V100R026C01SPC300 Common Criteria for Information Technology Security Evaluation, Parts: 1 – 5, CC:2022, Revision 1. Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, CEM:2022, Revision 1. EAL3 augmented with ALC_FLR.2
Evaluation Technical Report (ETR) Reference	Huawei_NCE-ETR HUAWEI iMaster NCE Security Services version V100R026C01SPC300 ETR, Version 1.1
CB identification	DEKRA Testing and Certification S.A.U. EUCC CB Body Number at ENISA: CB 3095
Author	Dariusz Rogowski
Date	30/10/2026
EUCC APPLICANT INFORMATION	
Applicant identification	Huawei Technologies Co., Ltd.
Manufacturer	Huawei Technologies Co., Ltd.
ITSEF INFORMATION	
ITSEF Identification	DEKRA Testing and Certification S.A.U. (ITSEF-2024-01) C/ Severo Ochoa, 2 y 6. Parque Tecnológico de Andalucía; 29590 Campanillas (Málaga) Body Number at ENISA: ITSEF 3095

CONTENT

1. Executive Summary 3

2. Bibliography and Acronyms 5

Bibliography 5

Acronyms 5

3. Evaluated ICT product 7

4. Security Services 9

5. Assumptions and Clarification of Scope 11

6. Architectural Information 12

7. Supplementary Cybersecurity Information 13

8. ICT Product Testing 14

9. Certificate Holder's Lifecycle Management Processes and Production Facilities 16

10. Evaluation Results 18

Evaluated Configuration 18

Summary of Evaluation Activities 18

Usage of the TOE 20

11. Information of the Certificate 21

12. Summary of the Security Target of the ICT Product 22

13. Mark and Label 23

1. Executive Summary

This document is the Certification report of the certification of the TOE Name: **HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100)** version **V100R026C01SPC300** developed on the basis of the Evaluation Technical Report [ETR] **HUAWEI iMaster NCE Security Services version V100R026C01SPC300 ETR, Version 1.1**.

This report is published together with the corresponding TOE EUCC certificate.

The TOE (CloudSOP)[1] is a next-generation OSS platform focused on information and communications technology (ICT) integration. The TOE provides platform security capability components. Based on service requirements, service functions are further developed on the CloudSOP platform. Products developed based on the CloudSOP platform have the same security capability components.

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

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

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

The major security features of the TOE are: User management, Authentication, Access control, Communication security, User session management, Auditing, Security management functions, Cryptographic functions. A detailed description of the security functionality is included in section **7. Security Requirements for the TOE** of the [ST].

The following provides a summary of threats and organizational security policies (OSPs) addressed by the evaluated ICT product as documented in the [ST]:

- **Threats:**

  Threat agents are defined as: an external attacker who is not a user of the TOE; an unauthorized user of the TOE, who gains unauthorized access to the TOE, and an eavesdropper, who has access to communication channels through which the Operations and maintenance (O&M) data and TSF data are transferred.

  The identified threats are:

  - Unauthenticated Access: An attacker (unauthenticated person) may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
  - Unauthorized Access: An unauthorized user who gains unauthorized access to the TOE and compromises the confidentiality and integrity of the TSF and O&M data. The user also performs unauthorized operations on Network Elements (NEs) through the TOE.
  - Eavesdrop: An eavesdropper (remote attacker) in the management network served by the TOE, who is able to intercept, modify, or re-use information assets that are exchanged between the TOE and NEs, between the NCE Client and TOE, and between the TOE and OSS/ service orchestrator/ service application.

[1] In manufacture internal maintenance the TOE refers to "CloudSOP".

- **Organizational Security Polices (OSPs):**

  Since the entire motivation for the defined security functionality is based on countermeasures against explicitly listed threats, **no OSPs** are defined.

The evaluated ICT product usage is recommended given that there are not exploitable vulnerabilities for the evaluated ICT product under its operational environment. The following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the evaluated ICT product in a proper manner.
- The user guidance must be read and understood in order to operate the evaluated ICT product in an adequate manner according to the [ST].
- The fulfilment of the assumptions indicated in the section Assumptions and Clarification of Scope of this document is a key point as it implies evaluated ICT product environment configurations that leave some potential vulnerabilities out of the scope.

The evaluation was conducted by the ITSEF DEKRA Testing and Certification S.A.U. and was finished on 23/10/2026 with **PASS** verdict.

The evaluation was conducted in accordance with the Common Criteria (CC) standard, version 2022, Revision 1 [CC2022].

The evaluation activities performed during the evaluation correspond to an assurance level of **EAL3 augmented with ALC_FLR.2** and with **AVA_VAN.2** as specified in [CC2022p3] and [CEM2022].

The certification results apply only to the product version specified in the certificate, subject to the conditions set out in this Certification Report.

The patch management is out of the scope of the evaluation.

Considering that all evaluation activities have been conducted in accordance with the Common Criteria requirements and have resulted in PASS, the Technical Reviewers' Team issues the following recommendation regarding the certification decision:

Recommendation on Certification Decision		
Recommendation of the Technical reviewer's team	**POSITIVE**	Certificate validity period: 5 years

2. Bibliography and Acronyms

Bibliography

[CC2022p1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2022, Revision 1
[CC2022p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 2022, Revision 1
[CC2022p3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 2022, Revision 1
[CC2022p4]	Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. Version 2022, Revision 1
[CC2022p5]	Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements. Version 2022, Revision 1
[CEM2022]	Common Methodology for Information Technology Security Evaluation. Version 2022, Revision 1
[CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[SotA]	EUCC SCHEME DRAFT STATE-OF-THE-ART DOCUMENT. ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME. Version 1.6c, July 2025
[ST]	CC HUAWEI iMaster NCE Security Services Security Target, Version 2.4, 23/10/2026.
[VUL1]	https://www.huawei.com/en/psirt/vul-response-process.
[VUL2]	Huawei Vulnerability Management White Paper.
[ETR]	HUAWEI iMaster NCE Security Services version V100R026C01SPC300 ETR, Version 1.1, 23/10/2026.

Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
CB	Certification Body
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
NE	Network Element
O&M	Operations and maintenance
OSP	Organizational Security Policy

PP	Protection Profile
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

3. Evaluated ICT product

3.1. Evaluated ICT product	
Name of the evaluated ICT product	HUAWEI iMaster NCE Security Services of NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (V100R025C10SPC100); NCE-Campus (V300R025C10SPC100); and SecoManager (V500R25C10SPC100), version V100R026C01SPC300
Enumeration of the ICT product's components that are part of the evaluation	1. iMasterNCE-FAN_V100R025C00SPC100_OMP_linux-aarch64.zip 2. iMasterNCE-FAN_V100R025C00SPC100_SRM_linux-aarch64.7z 3. iMasterNCE-FAN_V100R025C00SPC100_CloudSOPCloudService_linux-aarch64.7z 4. iMasterNCE-FAN_V100R025C00SPC100_CoreBase_linux-aarch64.7z 5. CC HUAWEI NCE Security Services AGD_PRE, v1.5 6. CC HUAWEI NCE Security Services AGD_OPE, v1.9 7. iMaster NCE V100R025C10 Product Documentation (Project Deployment & System Maintenance, Arm), v02 8. iMaster NCE-FAN V100R025C10 Product Documentation, v02
Version number of the ICT product's components	V100R025C00SPC100 for the above items 1, 2, 3, 4. 1.5 for AGD_PRE guidance 1.9 for AGE_OPE guidance 02 for the above items 7, 8
ST reference	CC HUAWEI iMaster NCE Security Services Security Target, Version 2.4, 23/10/2026
CC / CEM Version and Assurance Level	[CC2022] / [CEM2022] EAL 3 augmented with ALC_FLR.2 (AVA_VAN.2)
Identification of additional requirements to the operating environment of the certified ICT product	The TOE Version V100R026C01SPC300 identifies the specific software build of the TOE as deployed on the reference product NCE-FAN V100R025C10SPC100. The TOE can be deployed on NCE-IP, NCE-T, NCE-FAN, NCE-FAN Analyzer, NCE-Super, NCE-Fabric, NCE-CampusInsight, NCE-FabricInsight (all V100R025C10SPC100), NCE-Campus (V300R025C10SPC100) and SecoManager (V500R25C10SPC100).
Name and contact information of the holder of the EUCC certificate	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China support@huawei.com https://www.huawei.com
Patch management procedure included into the certificate	N/A

Vulnerability handling and Disclosure procedures / assurance continuity	https://www.huawei.com/en/psirt/vul-response-process [VUL1] Huawei Vulnerability Management White Paper [VUL2]
Link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided	On the page below under the link: Product Cybersecurity Information: https://carrier.huawei.com/en/products/fixed-network/imaster-nce-fbb

3.2. TOE Deliverables	
Component	**Description**
iMasterNCE-FAN_V100R025C00SPC100_OMP_linux-aarch64.zip	Includes the TOE Service packages: – SM-26.455.703-euler_arm64.zip – AuditLog-26.455.644-euler_arm64.zip – CloudSOPJavaFrameworks-26.455.620-euler_arm64.zip – MCTools-26.455.641-euler_arm64.zip
iMasterNCE-FAN_V100R025C00SPC100_SRM_linux-aarch64.7z	Includes the TOE Service package: – SMLogLic-26.455.994-euler_arm64.zip
iMasterNCE-FAN_V100R025C00SPC100_CloudSOPCloudService_linux-aarch64.7z	Includes the TOE Service package: – MinApiMgr-26.455.690.zip
iMasterNCE-FAN_V100R025C00SPC100_CoreBase_linux-aarch64.7z	Includes the TOE Service package: – SnbCertMgmt-26.455.683-euler_arm64.zip
CC HUAWEI NCE Security Services AGD_PRE, v1.5	Document describes the procedures of secure acceptance of the product in accordance with the delivery procedures defined for the product. This document also describes the steps for secure installation of the product and for the secure preparation of the operational environment. As the TOE cannot be independently installed and deployed, this document uses NCE-FAN as the deployment environment for the TOE.
CC HUAWEI NCE Security Services AGD_OPE, v1.9	The document describes how to manage and maintain the TOE after completing installation and commissioning in the operational environment. Document explicitly explains how to use the TOE's security functions for each role and fulfil AGD_PRE requirements.
iMaster NCE V100R025C10 Product Documentation (Project Deployment & System Maintenance, Arm), v02	The document includes details about the management plane functions. Documentation in .hdx format. Information: Users can login the HUAWEI support website to read all the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.
iMaster NCE-FAN V100R025C10 Product Documentation, v02	The document describes details about the O&M plane functions. Documentation in .hdx format. Information: Users can login the HUAWEI support website to read all the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.hdx, user can download the *.hdx reader from the same website.

4. Security Services

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

In the northbound direction, the TOE provides Web portals and northbound interfaces for O&M personnel, OSS, service orchestrator and service application. In the southbound direction, it provides some common configuration and management capabilities for Huawei network devices.

The TOE also interconnects with external NTP servers, SFTP servers, AAA authentication servers, Syslog servers, CA servers, SMS/SMTP servers and CAS/SAML SSO.

The iMaster NCE product is logically divided into two parts:

1. The TOE responsible for the security functions.
2. The Non-TOE Software responsible for the general business logic and network management functions.

Figure 1 shows an overview of the TOE parts:

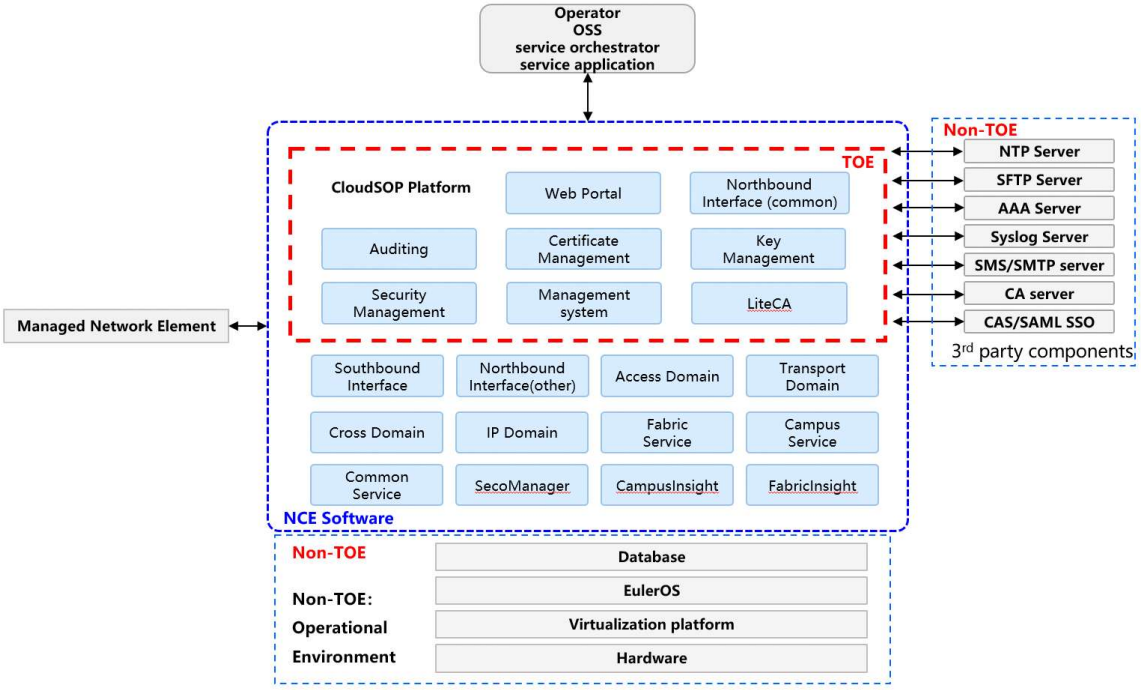


Figure 1. TOE overview [ST]

The major security features of the TOE that were subject to evaluation are:

User Management

On the management plane, and O&M plane, the TOE provides user management based on role management. On the management plane, it has the default user groups including Administrators, SMManagers, Monitors and Operators, while on the O&M plane, it has the default user groups like Administrators, SMManagers, NBI User Group, Maintenance Group, Operator Group. The TOE also allows admin and the SMManagers to create custom user-defined User Group on all planes.

Authentication

The TOE authenticates all users who access the TOE by username and password. The TOE provides a local authentication mode on the management plane, the O&M plane. The TOE optionally provides authentication credentials obtained from an external AAA in the IT environment on the O&M plane.

Access Control

The TOE supports admin and SMManagers to grant permissions to users by means of security management. Then users can access and perform operations on the TOE and NEs based on their permissions. The TOE offers a feature access control list (ACL) based on IP addresses for controlling which terminals can access the TOE.

Communication Security

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

User Session Management

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

Auditing

The TOE generates audit logs for security-relevant management and stores the logs in the database. Logs record routine maintenance events of the TOE. For security purposes, the TOE provides security logs, operation logs and system logs.

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

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

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

The query and filter functions are provided on the graphical user interface of the NCE Client, which allow authorized users to inspect audit logs.

Security Management Functions

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

Cryptographic Functions

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

The vulnerability handling policy of the manufacturer is described in [VUL1], [VUL2].

The assurance continuity policy will follow [EUCC] regulation.

The patch management is out of the scope of the evaluation.

5. Assumptions and Clarification of Scope

The assumptions defined in the Security Target [ST], as well as certain aspects of the identified threats and organisational security policies, are not addressed by the TOE itself. These aspects result in specific security objectives and measures that must be implemented by the operational environment.

The TOE is assured to provide effective security measures in a cooperative, non-hostile environment, provided that it is correctly installed, managed, and used. The following specific conditions are assumed to exist in the environment where the TOE is employed:

Assumption	Description
A.PhysicalProtection	It is assumed that the TOE and its operating environment (i.e. the complete system including the device hardware and attached peripherals) are properly protected to prevent unauthorized physical access. It is assumed that only Administrators and non-Administrators with explicit approval by the Administrator(s) are authorized to physically access the TOE and its operational environment. The underlying hardware and firmware that support the running of the TOE are trusted and can support the secure running of the TOE.
A.NetworkSegregation	It is assumed that the network interfaces of the server and TOE clients will be accessed only through the subnet where the TOE host is installed. The subnet is separated from the public network.
A.AdministratorBehaviour	It is assumed that the super user admin, a user that belongs to the SMManagers and Administrators groups and the users of the underlying operating system and operators authorized by the administrator to perform security-related operations will behave correctly and will not perform any harmful operation on the TOE.
A.NTP	It is assumed that operating environment will provide an accurate time source, in order to ensure normal operations of the TOE.
A.NetworkElements	It is assumed that the managed network elements are trusted and can support the Security connection with the TOE.
A.Components	It is assumed that the 3rd party components (NTP server, SFTP server, AAA server, syslog server, SMS/SMTP server, CA server and CAS/SAML SSO) are considered trusted and will not attack the TOE. For RADIUS authentication deployments, it is assumed that the RADIUS server supports the reception and processing of fragmented RADIUS authentication requests. It is assumed that the OSS/Service Orchestrator/Service application are considered trusted and will not attack the TOE. It is assumed that the NCE Client are considered trusted and will not attack the TOE.
A.TrustedPlatform	It is assumed that the platform including EulerOS, GaussDB, hardware and virtual machine used by the TOE is trusted, and is properly hardened by the Administrator of the customer with administrator rights. The platform provides a security domain for the TOE free from tampering by other programs on the same platform.

The TOE is not intended to counter threats outside the assumptions and operational environment defined in the Security Target [ST].

The certification applies exclusively to the evaluated TOE configuration and to the security functionality explicitly described in the [ST].

6. Architectural Information

The structure of the TOE in terms of subsystems and their identification is presented in Figure 2.

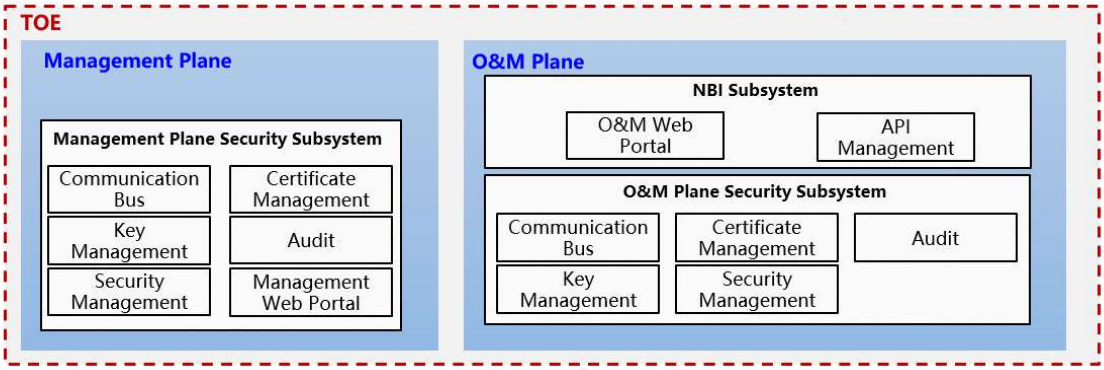


Figure 2. TOE subsystems

The whole functionality of the TOE is deployed into two different planes called **O&M Plane** and **Management Plane**. The management plane refers to the plane that manages the TOE software and hardware resources. The O&M Plane is composed by **NBI Subsystem**, **O&M Plane Security Subsystem**, and O&M Subsystem (outside the TOE). The Management Plane is composed by **Management Plane Security Subsystem** and Management Subsystem (outside the TOE).

Management Plane Security Subsystem provides the services platform for TOE, and has the security-related functions including authentication, authorization, audit log, session management and security management on the management plane.

NBI Subsystem provides open interfaces to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service applications. It is responsible for establishing a secure channel with the upper-layer application system.

O&M Plane Security Subsystem provides the services platform for TOE, and has the security-related functions including authentication, authorization, audit log, session management and security management on the O&M plane.

7. Supplementary Cybersecurity Information

The supplementary cybersecurity information required under Article 55(1) of Regulation (EU) 2019/881 is made publicly available by the manufacturer through the following product webpage and its linked documentation, under **Resources → Product Cybersecurity Information**:

https://carrier.huawei.com/en/products/fixed-network/imaster-nce-fbb

The supplementary cybersecurity information document is available at:

https://carrier.huawei.com/~/media/CNBGV2/download/adn/cybersecurity-Information.pdf

The following points provide details on where and how to access the published information addressing each of the requirements of Article 55(1).

1. Guidance for secure configuration, installation, deployment, operation and maintenance.

   The supplementary information document links to the HUAWEI iMaster NCE Security Services User Guide, Issue 1.0, dated 21 August 2026. The TOE name and identification are consistent with the ST. Sections 2–4 cover the secure operational environment, deployment, installation, software integrity verification, configuration, operation and maintenance.

   https://carrier.huawei.com/~/media/CNBGV2/download/adn/cybersecurity-guidelines.pdf

2. Security support period, including cybersecurity-related updates.

   The supplementary information document states that cybersecurity support for the Huawei iMaster NCE Series will be aligned with the validity period of the EUCC certificate. For further information on maintenance and cybersecurity-related updates, it provides the contact address **support@huawei.com** and references Huawei's product lifecycle policy:

   https://www.huawei.com/en/declarations/lifecycle-management-letter

3. Contact information and accepted methods for reporting vulnerabilities.

   The referenced Huawei PSIRT webpage provides **psirt@huawei.com** as the vulnerability reporting channel, together with reporting instructions, a template and a PGP public key for encrypted submissions.

   https://www.huawei.com/en/psirt/report-vulnerabilities

4. Public vulnerability repositories and relevant cybersecurity advisories.

   The supplementary information document references EUVD, specifying “Huawei iMaster NCE” as the search term:

   https://euvd.enisa.europa.eu/

The certificate holder is responsible for keeping this information electronically available and updated as necessary at least until certificate expiry, in accordance with Article 55(2).

8. ICT Product Testing

The certificate is issued by **DEKRA Testing and Certification S.A.U. EUCC CB (3095)**, under the authority of the Spanish NCCA (ANCC CCN-Centro Criptológico Nacional).

The evaluation was performed by **the ITSEF DEKRA Testing and Certification S.A.U.**

The evaluation activities performed for an assurance level of **EAL3 augmented with ALC_FLR.2**, as specified in [CC2022p3] and [CEM2022], are summarized in the following table:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary ADV_TDS.2 Architectural Design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization controls ALC_CMS.3 Implementation representation CM coverage ALC_DEL.1 Delivery procedure ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability Analysis

No state-of-the-art documents or additional security evaluation criteria were applied in this evaluation.

The [ST] does not claim conformance to any PP.

Independent testing was performed by the evaluator to verify that the TOE operates as specified, following an SFR-oriented approach. The evaluator, as part of the independent tests, repeated a sample of the developer tests, following his procedures to gain confidence in the results obtained. Next, the evaluator devised, based on the developer tests, their own test scenarios to operate the TOE in a different manner. The main objective of the tests was to check that the security functional requirements defined in [ST] are implemented as expected, and whether the subsystems behave as defined in the TOE design documentation, and whether TSFIs definitions are consistent with the TOE functional specification.

In addition, a vulnerability analysis was conducted based on publicly available sources, the TOE documentation, and its evaluated configuration. An independent search for potential vulnerabilities did not identify any applicable vulnerabilities or plausible attack paths exploitable with a Basic attack potential. During the evaluation activities development, it has been recorded several aspects of concerns which have been considered in the penetration tests design. All potential vulnerabilities identified were tested through the penetration testing which confirmed the TOE is resilient against attackers with the BASIC attack potential.

9. Certificate Holder's Lifecycle Management Processes and Production Facilities

This section summarizes the configuration management system applied by the holder of the certificate for the identification of the configuration items, its versioning method and change control.

The scope of the Configuration Management System covers: the TOE, Parts of the TOE, Developer evidence, Implementation representation. Configuration management procedures include activities of creation, modification or deletion of a configuration item. Configuration management documentation defines the roles and responsibilities of individuals required to perform operations on individual configuration items.

Huawei Technologies defined and employed the life-cycle model which encompasses the procedures, tools and techniques used to develop and maintain TOE subject to CC security evaluation projects. Aspects of the process that have been covered by the model include design methods, review procedures, project management controls, change control procedures, test methods and acceptance procedures.

Configuration Management Tools used for CC:

- CodeHub is used for code storage. The source code of Huawei R&D developed code and third-party open source software and build tools is available in CodeHub.
- D-Box is used mainly for internal documentation management. It can be used to set permissions on configuration items and configure baseline items.
- CMC (Artifactory) is mainly used to store released versions. The version manager group has permission to write the version. When the process is complete, the system automatically changes the permissions to read-only.
- Defect Trace System (DTS) is used for tracking the list of defects. A DTS ticket includes the version information, module or sub-system information, description of the defect, urgency, and other information. Each defect flow has several states, for example, created, project manager reviewed, implemented, implementation reviewed, regression testing, defect recognition.

TOE Versioning

The VRC tag is the product version and stands for **Version vvv Release rrr C cc**. When referencing the TOE, the labels or references of the documents may use the VRC format (for example, V100R026C01). If the version needs to be released again due to certain reasons, the patch version number **SPC sss** (for example, V100R026C01SPC300) is used. A patch is a software unit designed to fix defects in a product version. It is used to correct errors (including code, design, and feature errors) from the perspective of customers. It is prohibited to use patches to meet new customer requirements.

Identification of the Documentary Evidences

Naming rule of product documents:

- Internal product name or product name + White space + Product version + White space + (Subsystem name/module name/requirement description) + White space + Documentation category + (Feature name).
- Product Document Example: CloudSOP_V100R026C01 Product Description.chm

CC certification documents are identified as follows:

- CC + White space + HUAWEI + White space + Product name + White space + Documentation category + Document version
- Sample: CC HUAWEI iMaster NCE Security Services Security Target V1.0
- CC Certification document Example

Category	Evidence Name
ASE	CC HUAWEI iMaster NCE Security Services Security Target V1.0
ADV	CC HUAWEI iMaster NCE Security Services Security Architecture V1.0
AGD	CC HUAWEI iMaster NCE Security Services AGD_OPE V1.0

Site visits

A site visit has been performed in the vendor facilities located at:

Company name: HUAWEI TECHNOLOGIES CO., LTD.

Address: Huawei Dongguan research center,Xiliu Beipo Village,Huanhu Road,High- tech Industrial Development Zone,Songshan Lake,Dongguan,Guangdong Province, China

- Building V5, Huawei Xi'an research center, No.127 Jinye Road, Xi'an High-Tech Development District, Xi'an, Shaanxi Province, China
- Huawei Machine ltd, No.2 Xincheng Road, Songshan Lake, National High-tech Industrial Development Zone, Dongguan, Guangdong Province
- Huawei Gui'an Data Center, No.1 Shugu Avenue, Pingba District, Anshun City, Guizhou Province
- Block T, Huawei Tuanbowa Campus, No.1 Taizhong Road, Songshan Lake, National High-tech Industrial Development Zone, Dongguan, Guangdong Province
- Huawei Suzhou research center, Sangtian Island, No. 9 Jiangyun Road, Suzhou Industrial Park,Suzhou, Jiangsu Province.

10. Evaluation Results

The ITSEF produced and provided the Evaluation Technical Report [ETR] and companion partial reports of each activity (ASE, ADV, ALC, AGD. ATE and AVA) according to the requirements of the [EUCC] and the Common Criteria [CC2022] and the Common Evaluation Methodology [CEM2022].

The evaluation of the ICT product, has confirmed that it meets the requirements for assurance level 'Substantial' as defined in Article 4 of the EUCC Implementing Regulation and Article 52 of Regulation (EU) 2019/881 [EUCC].

The AVA_VAN.2 component indicates that the product was evaluated to resist attacks from attackers with a BASIC attack potential.

Based on the review of the evaluator's analysis and conclusions for the ASE, ALC, AGD, ADV, ATE, and AVA activities, it can be confirmed that the evaluation was conducted in accordance with the Common Criteria [CC2022] requirements and the Common Evaluation Methodology [CEM2022].

Evaluated Configuration

The evaluated configuration consists of the TOE, HUAWEI iMaster NCE Security Services, version V100R026C01SPC300, deployed on NCE-FAN V100R025C10SPC100, which serves as the reference product and provides the operational environment for the TOE evaluation, as defined in the [ST].

This configuration is established by following the guidance provided with the TOE and ensuring that all security objectives for the operational environment specified in the [ST] are fulfilled.

As detailed in the [ETR], the evaluator tested the TOE using this reference configuration.

Summary of Evaluation Activities

The evaluation resulted in a PASS verdict for all assurance components listed in section 7 of the report [ETR] and claimed in the Security Target [ST] for the TOE. A summary of the evaluation activities is provided below.

ASE:

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target and its components. The identified threats, security objectives, and security requirements are appropriately addressed, and the TOE description is both accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements for EAL3 augmented with ALC_FLR.2. No issues or deviations were identified that could impact the assurance of the TOE.

ALC:

The evaluation results demonstrate that the TOE's lifecycle processes, covering configuration management, delivery, and related controls, are clearly defined, properly implemented, and aligned with the required assurance level. The submitted evidence supports traceability of changes and the secure handling of the TOE throughout its lifecycle.

Additionally, during the site visit activities the evaluator examined configuration management system, delivery procedures, development security in the means of physical, logical and personnel measures and confirmed they are applied, operated and sufficient to protect confidentiality and integrity of the TOE.

The evaluation findings demonstrate sound implementation of flaw remediation procedures by the TOE developer. Flaw tracking model describes actions taken by the developer from the time each suspected security flaw is reported to the time it is resolved. Product Vulnerability Response Process describes the procedures to track all reported security flaws in each release of the TOE. The evaluation results confirmed the flaw remediation procedures describe the means of providing the TOE users with the necessary information on each security flaw with its description, corrective action, and any associated guidance on implementing the correction, the methods the user can report security flaws, enquire about the status of security flaws, or request corrections to flaws.

A unique reference is clearly defined to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Accordingly, the ALC activities satisfy the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified that could compromise the TOE's security.

AGD:

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure installation, configuration, and operation of the TOE within its intended environment. The guidance effectively helps prevent common misconfigurations and promotes correct usage.

The preparative procedures describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures, and all the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives defined in [ST].

The operational user guidance describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

The operational guidance and related evidence documentation identify all possible modes of operation of the TOE, their consequences and implications for maintaining secure operation.

Therefore, the AGD activities fulfil the assurance requirements for EAL3 augmented with ALC_FLR.2, with no issues or deviations identified.

ADV:

The findings confirm that the design documentation provides sufficient detail to understand the TOE's architecture and security-enforcing functions. The evidence demonstrates clear traceability between the security requirements and the TOE design.

The security architecture evaluation demonstrated security domains maintained by the TSF, initialization process preserves security, TSFs are able to protect themselves from tampering and bypass attacks.

The functional specification evaluation demonstrated the presentation of the TSFI completely and accurately describes SFR-enforcing actions associated with the SFR-enforcing TSFIs.

The TOE design evaluation demonstrated the structure of the entire TOE is described in terms of subsystems.

Accordingly, the ADV activities meet the assurance requirements for EAL3 augmented with ALC_FLR2, with no issues or deviations identified.

ATE:

The testing evidence provided by the developer has been thoroughly reviewed and verified as complete, demonstrating correct implementation of the TOE's specified security functions. This includes validation of cryptographic operations, user data protection, and other security measures to ensure compliance with the defined requirements.

The evaluator conducted independent testing to further verify the accuracy and reliability of the developer's claims, executing a comprehensive set of tests that confirmed the TOE operates as intended, with no failures or security vulnerabilities identified. The testing approach for the TOE behaviour description demonstrates the interactions among subsystems as described in the TOE design.

As a result, the independent testing confirms that the TOE complies with all relevant security requirements specified for the evaluation. The testing process, encompassing both the developer's evidence and the evaluator's independent tests, has been comprehensive and thorough. No issues or deviations were identified during the evaluation, and the testing activities fully satisfy the assurance requirements for EAL3 augmented with ALC_FLR.2.

AVA:

The evaluator performed a vulnerability analysis to identify publicly known vulnerabilities and assess whether any could be exploited with a BASIC attack potential. This assessment included an in-depth analysis of the TOE itself, as well as any third-party components or libraries it depends on. Publicly known vulnerabilities such as those documented in security databases and related to the TOE's software components were considered.

The evaluator analysed the [ST], guidance documentation, functional specification, TOE design and security architecture description during evaluation evidence activity to identify areas of concern for potential vulnerabilities. The testing process involved penetration tests using commonly known methods and techniques to evaluate the TOE's resistance to potential exploitation.

Beyond assessing known vulnerabilities, the evaluation also examined the TOE's resilience within its defined operational environment. The analysis confirmed that the TOE maintains robustness against such attacks, with no significant vulnerabilities identified that could undermine its security.

Consequently, the AVA activities were performed in full compliance with the assurance requirements for EAL3 augmented with ALC_FLR.2, providing a reasonable level of confidence in the TOE's resilience against attackers with the BASIC attack potential.

Usage of the TOE

The use of the certified ICT product is recommended, as no exploitable vulnerabilities have been identified within the defined operational environment. The following usage recommendations apply:

- The installation procedures provided in the documentation shall be strictly followed to ensure the correct download and proper installation of the evaluated version of the ICT product.
- The user guidance shall be carefully read and understood to ensure that the product is operated in accordance with the Security Target [ST].
- Compliance with the assumptions specified in section **Assumptions and Clarification of Scope** is essential, as these define the evaluated operational environment and imply that certain potential vulnerabilities are considered out of scope.

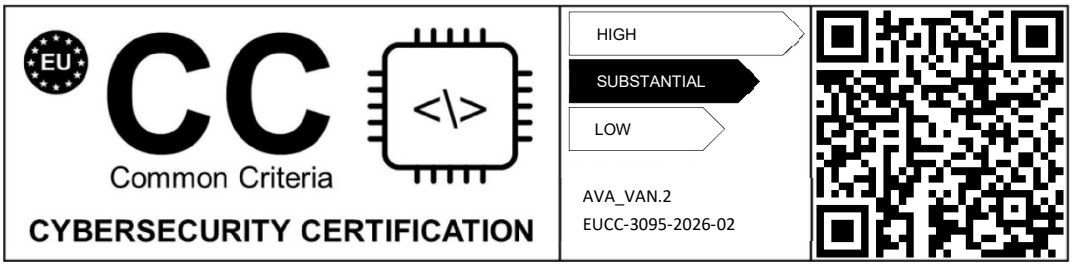
11. Information of the Certificate

Date of Issuance	30/10/2026
Period of Validity	Valid for five years from the date of issuance *The certificate is valid for five (5) years from the date of issuance, inclusive, and remains valid until the end of 29/10/2031, unless suspended or withdrawn earlier*
Unique Identifier of the Certificate	EUCC-3095-2026-02 version 1.0
Scheme Name	(EU) 2024/482 - EUCC
Certification Body Accreditation Reference Number	DEKRA Testing and Certification S.A.U. EUCC CB ENAC´s Accreditation number **134/C-PR337** ENISA´s Body number: **3095**
Certificate Authorising Participant	ANCC CCN-Centro Criptológico Nacional

12. Summary of the Security Target of the ICT Product

For publication purposes, the Security Target of the TOE [ST] “CC HUAWEI iMaster NCE Security Services Security Target, Version 2.4, 23/10/2026” is provided as a separate document together with this Certification Report.

13. Mark and Label



Signature: Dariusz Rogowski **EUCC CB Technical Reviewer** DEKRA Testing and Certification S.A.U.	Signature: Alejandro Muñoz del Rey **EUCC CB Technical Manager** DEKRA Testing and Certification S.A.U.