Certification Report

HUAWEI iMaster NCE-T V100R021C10SPC202

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
D4 D Area Administration Building, Southern Factory of Huawei Technologies Co.,Ltd., No 6 Xincheng Avenue Songshan Lake Technology Industrial Park, Dongguan City, 523808
P.R.C.

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2200027-01-CR**

Report version: **1**

Project number: NSCIB-**2200027-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **08 September 2023**

Number of pages: **11**

Number of appendices: **0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the HUAWEI iMaster NCE-T V100R021C10SPC202. The developer of the HUAWEI iMaster NCE-T V100R021C10SPC202 is Huawei Technologies Co., Ltd. located in Dongguan, P.R.C. and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

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.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 08 September 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the HUAWEI iMaster NCE-T V100R021C10SPC202, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the HUAWEI iMaster NCE-T V100R021C10SPC202 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the HUAWEI iMaster NCE-T V100R021C10SPC202 from Huawei Technologies Co., Ltd. located in Dongguan, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei iMaster NCE-T	V100R021C10SPC202

To ensure secure usage a set of guidance documents is provided, together with the HUAWEI iMaster NCE-T V100R021C10SPC202. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE 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 TOE has the following features:

- User management: On the management plane, there is only one super user admin. On the O&M plane, the TOE provides user management based on the role management. It has the following default user groups: Administrators, SMManagers, NBI User Group, Maintenance Group, Operator Group, and Guests. It also defines user groups for different user roles.
- Authentication: The TOE authenticates all users who access the TOE by username and password. The TOE provides a local authentication mode both on the management plane and the O&M plane. The TOE optionally provides authentication decisions 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.
- 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.
- Security management function: 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 a number of strong cryptographic algorithms.

2.3 Assumptions and Clarification of Scope

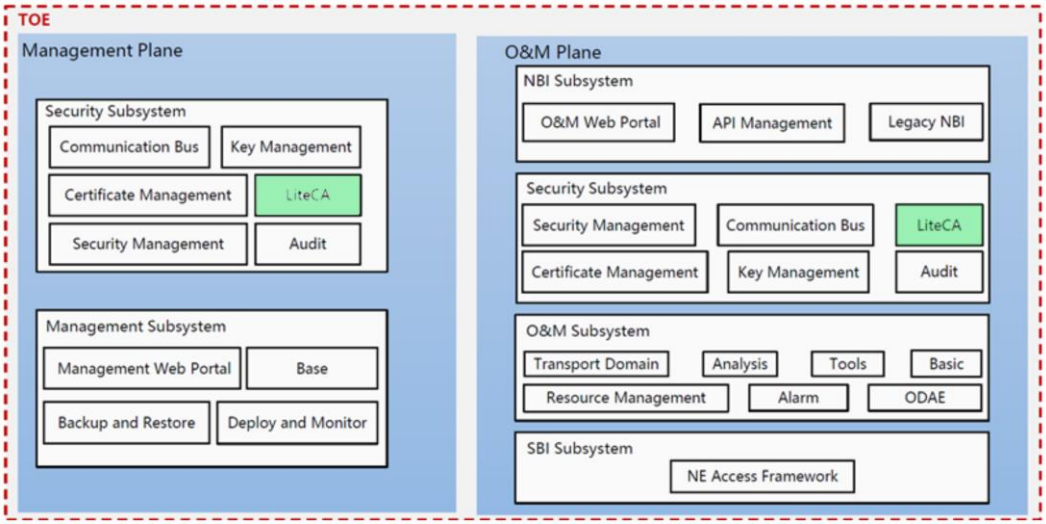
2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information



The TOE logical architecture consists of two independent planes, and each plane consists of a number of subsystems and modules:

- Management plane: the plane that is responsible to manage the TOE itself. It consists the following subsystems:
  - Security subsystem: responsible for providing the security features of the TOE (I&A, communication security, security management, certification management, key management, and audit logs).
  - Management subsystem: functional subsystem to perform management tasks of the TOE, such as performing the backup or monitoring the system usage.
- O&M plane: the plane that is responsible for providing main functionalities of the TOE, that is, managing the network elements (NE). It consists of the following subsystems:
  - NBI subsystem: providing north bound interface (e.g., CORBA, TL1, RESTful API) to the north bound Operation Support System (OSS).
  - Security subsystem: responsible for providing the security features of the TOE (I&A, communication security, security management, certification management, key management, and audit logs).
  - O&M subsystem: provides the business functionalities for the TOE to manage the network elements.
  - SBI Network: provides access channels and secure channels for the TOE and NEs to communicate in a protected manner.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
CC HUAWEI iMaster NCE V100R021C10 - Installation Guide, Dated 11 January 2023	V1.2
CC HUAWEI iMaster NCE V100R021C10 - Security Management Guide, Dated 09 January 2023	V1.2
iMaster NCE V100R021C10 Product Documentation (Project Deployment & System Maintenance, Arm), Dated 30 September 2022	02-C
iMaster NCE V100R020C10 Product Documentation (Project Deployment & System Maintenance, Arm), Dated 30 September 2022	04-C

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and TSFI to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS) to collect information about the TOE and identify potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was 2.5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- NCE-T V100R020C10SPC202

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 2 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number HUAWEI iMaster NCE-T V100R021C10SPC202.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the sites *[STAR]* [2].

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the HUAWEI iMaster NCE-T V100R021C10SPC202, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The CC HUAWEI iMaster NCE-T V100R021C10 - Security Target, Version 1.5, dated 10 January 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NBI	Northbound Interface
NSCIB	Netherlands Scheme for Certification in the area of IT Security
O&M	Operation and Maintenance
OSS	Operations Support System
PP	Protection Profile
SBI	Southbound Interface
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report Huawei iMaster NCE-T V100R021C10SPC202 – EAL4+, [22-RPT-1329], Version 2.0, Dated 13 June 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP]	Common Criteria Protection Profile for Network Device Management (NDhPP), Version 1.0, 2021-04-23, registered under the reference NSCIB-PP-0335832
[ST]	CC HUAWEI iMaster NCE-T V100R021C10 - Security Target, Version 1.5, dated 10 January 2023
[STAR_ Dongguan]	STAR Huawei Dongguan F1 Development site, [23-RPT-304], Version 2.0
[STAR_ Wuhan]	STAR Huawei Wuhan A6 Development site, [23-RPT-305], Version 2.0
[STAR_ Nanjing]	STAR Huawei Nanjing N5 Development site, [23-RPT-306], Version 2.0
[STAR_ Beijing]	STAR Huawei Beijing Q15 Development site, [23-RPT-307], Version 2.0
[STAR_ Xi'an]	STAR Huawei Xi'an V5&V6 Development site, [23-RPT-308], Version 2.0

(This is the end of this report.)