Certification Report

Huawei iMaster MAE V100R024C10SPC210

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-2400160-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400160-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**15 September 2025**
Number of pages:	**12**
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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 MAE V100R024C10SPC210. The developer of the Huawei iMaster MAE V100R024C10SPC210 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 centralized operation and maintenance (OM) for mobile network element management solution, provides external interfaces for interoperability with other systems. By providing automatic network OM capabilities, the TOE can implement automatic network management.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 15 September 2025 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 MAE V100R024C10SPC210, 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 MAE V100R024C10SPC210 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, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

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 MAE V100R024C10SPC210 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
Hardware	N/A	N/A
Software	MAE_V100R024C10SPC210_Access_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Deployment_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Jre_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Common_EulerOS-aarch64.zip MAE_V100R024C10SPC210_KPI_EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSP_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Evaluation_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Common_HD_EulerOS-aarch64.zip MAE_V100R024C10SPC210_Optimization_EulerOS-aarch64.zip iPowerStar_3.1.5.1_MAE12410-EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSF_EulerOS-aarch64.zip MAE_V100R024C10SPC210_TSF_CBB_EulerOS-aarch64.zip 5GtoBSuite_3.1.5.1_MAE12410-EulerOS-aarch64.zip MAE-OSMU_V100R024C10SPC210_EulerOS-aarch64_pkg.tar MAE-OSMU_V100R024C10SPC210_VNFLCM-IAASDeploy_EulerOS_pkg.tar	V100R024C10SPC210
Software Signature file	MAE_V100R024C10SPC210_Access_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Deployment_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Jre_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Common_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_KPI_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_TSP_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Evaluation_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Common_HD_EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_Optimization_EulerOS-aarch64.zip.p7s iPowerStar_3.1.5.1_MAE12410-EulerOS-aarch64.zip.p7s MAE_V100R024C10SPC210_TSF_EulerOS-aarch64.zip.p7s	V100R024C10SPC210

Delivery item type	Identifier	Version
	MAE_V100R024C10SPC210_TSF_CBB_EulerOS-aarch64.zip.p7s 5GtoBSuite_3.1.5.1_MAE12410-EulerOS-aarch64.zip.p7s MAE-OSMU_V100R024C10SPC210_EulerOS-aarch64_pkg.tar.p7s MAE-OSMU_V100R024C10SPC210_VNFLCM-IAASDeploy_EulerOS_pkg.tar.p7s	
Platform software	MAE_V100R024C10SPC210_CloudSOP_EulerOS-aarch64.zip	V100R024C10SPC210
Platform software signature file	MAE_V100R024C10SPC210_CloudSOP_EulerOS-aarch64.zip.p7s	V100R024C10SPC210

To ensure secure usage a set of guidance documents is provided, together with the Huawei iMaster MAE V100R024C10SPC210. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The major security features implemented by the TOE are:

- User management
- Authentication
- Access control
- IP-based ACL
- Communication security
- User session management
- Auditing
- Security management function
- Cryptographic functions

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

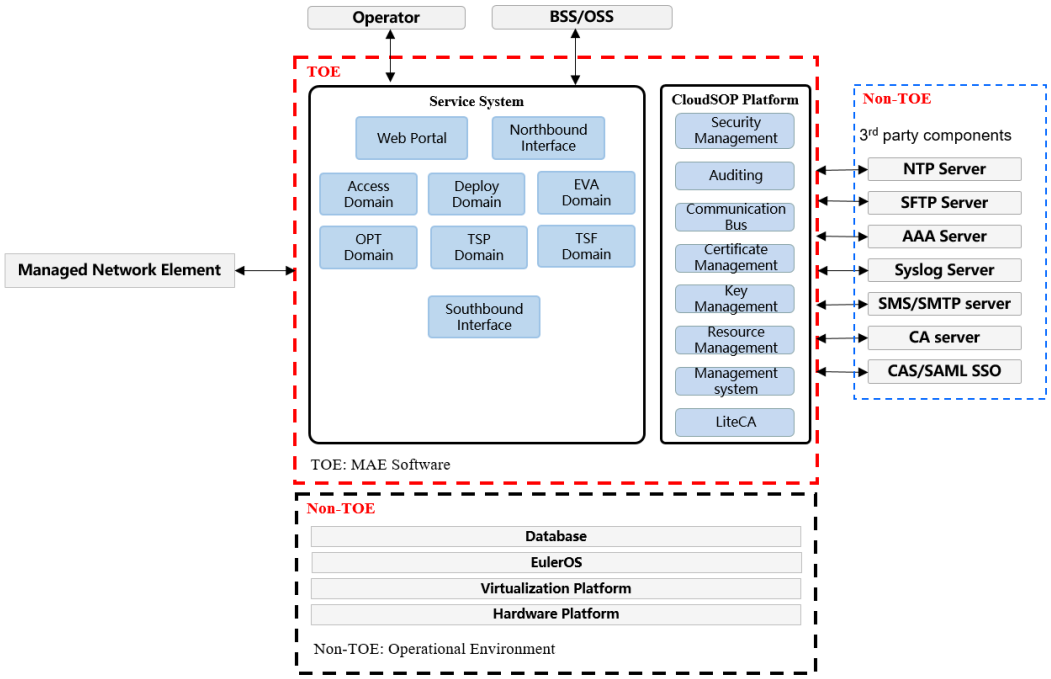
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

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 architecture can be depicted as follows:



2.5 Documentation

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

Identifier	Version
CC HUAWEI iMaster MAE V100R024C10 - Preparative Procedures.pdf, dated 25 June 2025	Product version: V100R024C10, Issue: 02,
CC HUAWEI iMaster MAE V100R024C10 - Operational user Guidance.pdf, dated 13 March 2025	Product version: V100R024C10, Issue: 02,
(For Customer)iMaster MAE Product Documentation (EulerOS, TaiShan)-(V100R024C10_*)(HDX)-EN.hdx, dated 11 July 2025	Product version: V100R024C10, Library Version: 07,
iPowerStar 3.1.5 Product Documentation *-EN.hdx, dated 28 March 2025	Product version: V100R024C10(iPowerStar 3.1.5), Library Version: 05,
5GtoB Suite 3.1.4 Product Documentation *-EN.hdx, dated 29 June 2024	Product version: V100R024C10(5GtoB Suite 3.1.4), Library Version: 02,
OSMU User Guide(EulerOS, TaiShan)(V100R024C10_*)(WORD)-EN.zip, dated 20 April 2024	Product version: V100R024C10, Issue: 06,
iMaster MAE V100R024C10SPC210 Release Documents(EulerOS, TaiShan)-EN.zip, dated 222 January 2025	Product version: V100R024C10SPC210,

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

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 were 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.

2.6.2 Independent penetration testing

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The evaluator tested the TOE in the following configuration:

- TOE version: V100R024C10SPC210

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

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 1 Site Technical Audit Report.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei iMaster MAE V100R024C10SPC210.

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

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

Based on the above evaluation results the evaluation lab concluded the Huawei iMaster MAE V100R024C10SPC210, 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]*.

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>.

3 Security Target

The CC HUAWEI iMaster MAE V100R024C10 -Security Target Version v 2.2, Dated 26 August 2025 *[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
NSCIB	Netherlands Scheme for Certification in the area of IT Security
OM	Operation and Maintenance
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 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report “Huawei iMaster MAE V100r024C10SPC210” – EAL4+, 25-RPT-318, Version 2.0, Dated 11 September 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	CC HUAWEI iMaster MAE V100R024C10 -Security Target Version v 2.2, Dated 26 August 2025

(This is the end of this report.)