Certification Report

Huawei iMaster MAE V100R020C10

Sponsor and developer:	***Huawei Technologies Co.,Ltd*** **No 6 Xincheng Avenue, Songshan Lake Technology Park** **Dongguan City 523808** **China**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0132795-CR**
Report version:	**1**
Project number:	**0132795**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**30 November 2020**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license 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, TÜV Rheinland Nederland 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, in order 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 authorized provided the report is reproduced in its entirety.

Recognition of the certificate

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

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei iMaster MAE V100R020C10. The developer of the Huawei iMaster MAE V100R020C10 is Huawei Technologies Co.,Ltd located in Dongguan, China 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 the software for managing mobile networks. It provides a centralized network management platform for supporting telecom operators in their long-term network evolution and shielding the differences between various network technologies. The TOE provides various OM solutions and meets various requirements, such as network deployment, network monitoring, network adjustment, and service management.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 24th of September 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 V100R020C10, 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 V100R020C10 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 provides 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 (Systematic flaw remediation).

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]*.

TÜV Rheinland Nederland 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. It should be noted that the certification results only apply 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 releasable 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 V100R020C10 from Huawei Technologies Co.,Ltd located in Dongguan, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	HUAWEI iMaster MAE	V100R020C10SPC210

To ensure secure usage a set of guidance documents is provided together with the Huawei iMaster MAE V100R020C10. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE is a centralized network management software. The MAE is located at the management and control layer of the cloud network. It can manage and control ubiquitous network devices such as global system for mobile (GSM), wideband code division multiple access (WCDMA), code division multiple access (CDMA), worldwide interoperability for microwave access(WiMAX), long term evolution (LTE). It provides open interfaces to quickly integrate with upper-layer application systems such as BSS and OSS. Various apps can be developed and customized to accelerate service innovation and achieve e-commerce-style operations.

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

2.3 Assumptions and Clarification of Scope

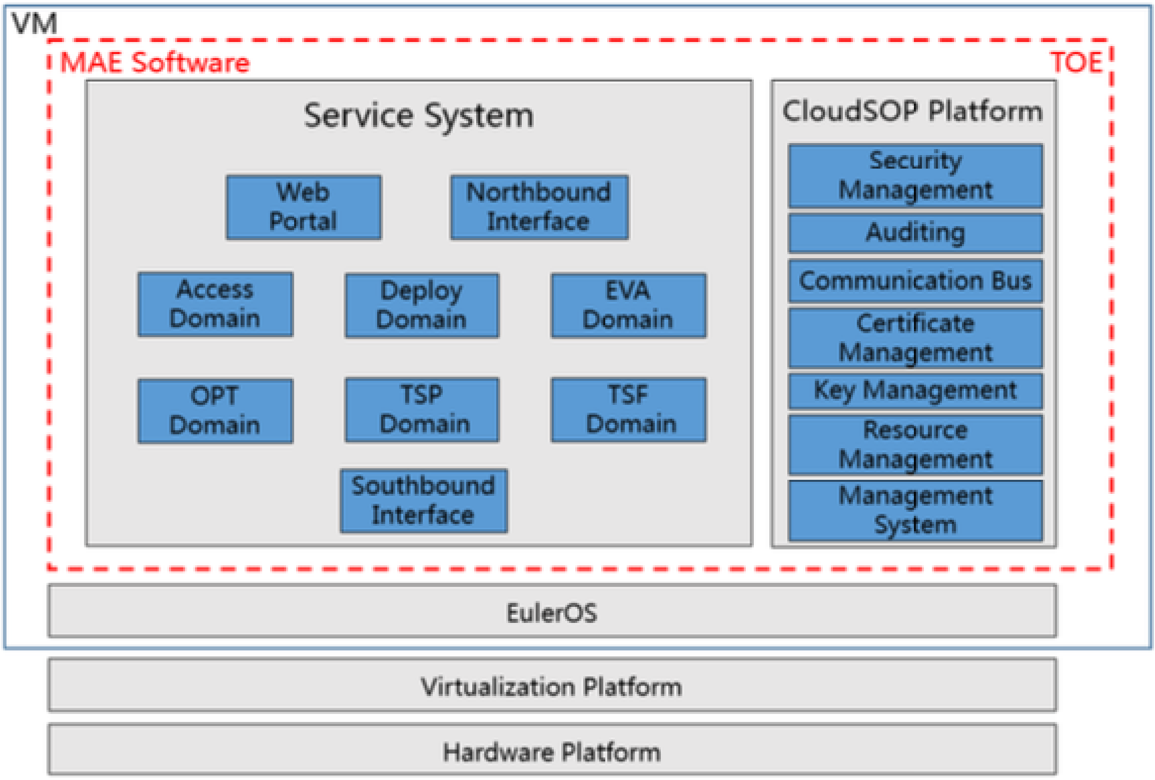
2.3.1 Assumptions

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.1 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



2.5 Documentation

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

Identifier
CC Huawei MAE Software V100R020C10 - AGD_OPE
CC Huawei MAE Software V100R020C10 - AGD_PRE

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

For the testing performed by the evaluators, the developer has provided samples and a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

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 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, Testssl.sh) 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 analysed, 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.

2.6.3 Test Configuration

The developer tested the TOE in the following configuration:

- MAE V100R020C10SPC210

2.6.4 Testing 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 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei iMaster MAE V100R020C10.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* and ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the Huawei iMaster MAE V100R020C10, 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 contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to 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. In order for the evolution of attack methods and techniques to be covered, he 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.

3 Security Target

The CC HUAWEI iMaster MAE V100R020C10 - Security Target, version 1.9, 2020-09-14 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NE	Network Element
NSCIB	Netherlands Scheme for Certification in the area of IT security
OM	Operation and Maintenance
OSS	Operations Support System
PP	Protection Profile
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 iMaster MAE V100R020C10SPC300, 20-RPT-742 [ETR] Huawei iMaster MAE V100R020C10 v4.0, 26 November 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] CC HUAWEI iMaster MAE V100R020C10 - Security Target, version 1.9, 2020-09-14.

(This is the end of this report).