TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

HUAWEI eSight 20.1.0

Sponsor and developer: **Huawei Technologies Co., Ltd.**
Administration Building, Huawei Industrial Base, Bantian, Longgang
Shenzhen 518129
People's Republic of China

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

Report number: **NSCIB-CC-0444182-CR**

Report version: **1**

Project number: **0444182**

Author(s): **Kjartan Jæger Kvassnes**

Date: **25 March 2022**

Number of pages: **11**

Number of appendices: **0**

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

TÜVRheinland®
Precisely Right.

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 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, 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, 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

The 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 eSight 20.1.0. The developer of the HUAWEI eSight 20.1.0 is Huawei Technologies Co., Ltd. located in People's Republic of 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 a software system based on a cloud platform providing cloud network management, located at the management and control layer of the cloud-based network. The TOE is an integrated Operation and Maintenance (O&M) management solution for enterprises. It centrally manages servers, storage devices, switches, routers, and firewalls and provides a diverse range of functions for enterprise ICT infrastructure, such as automatic configuration and deployment, visualized fault diagnosis, and intelligent capacity analysis. The TOE is a software solution which is deployed at the management and control layer of a cloud-based network.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 25 March 2022 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 eSight 20.1.0, 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 eSight 20.1.0 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).

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. 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 eSight 20.1.0 from Huawei Technologies Co., Ltd. located in People's Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei eSight	20.1.0

In the certified configuration, the TOE supports multi-node cluster with dual (network) plane deployment.

To ensure secure usage a set of guidance documents is provided, together with the HUAWEI eSight 20.1.0. For details, see section 2.5 "Documentation" of this report.

2.2   Security Policy

eSight can be deployed in a single-node system or in a cluster and provides open interfaces for interconnection and integration with upper-layer OSS or third-party systems. Simplified, automated, and intelligent O&M improve O&M efficiency.

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

- User management
- Authentication
- Access control
- 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 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
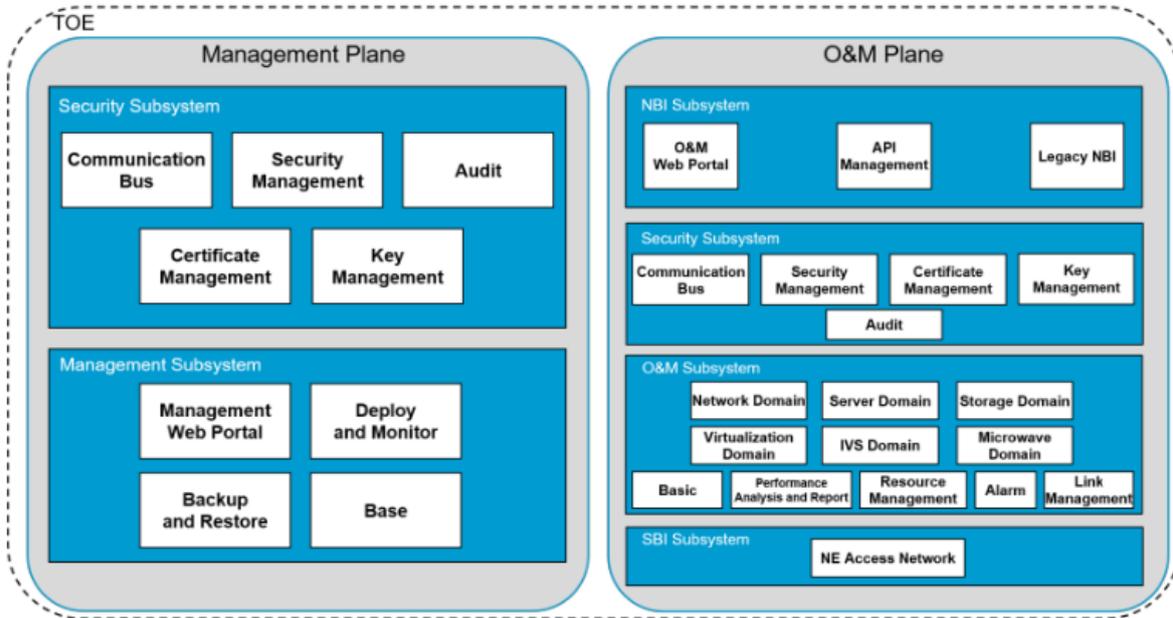
The TOE logical architecture consists of two independent planes, and each plane consists of a number of subsystems and modules:

- 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: Provides north bound interfaces (e.g. SNMPv3, RESTAPI, etc.) to the north bound device OSS (Operation Support System).
    - 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 subsystem: 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 eSight 20.1.0 Installation Guide, dated 7 January 2022	1.1
CC HUAWEI eSight 20.1.0 Security Management Guide, dated 14 January 2022	1.3
CC HUAW EI eSight 20.1 Product Documentation, dated 14 January 2022	0.9

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 test approach is summarized as follows:

- The test cases are divided into five chapters that cover:
  o   All TSFIs
  o   All Subsystems and subsystem interactions
- Four chapters map to the four TSFI categories
- One chapter maps to the cryptographic operations performed on the TOE

As all SFRs are tested, therefore the complete TSF is tested.

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 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.

The total test effort expended by the evaluators was 4 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3   Test configuration

For testing, eSight 20.1.0 deployed in multi-node cluster with single (network) plane.

The evaluator assessed that from testing perspective there was no difference whether the TOE is deployed in a single-plane or a dual-plane configuration as the network plane configuration is the configuration in the environment and has no effect on the operation of the TOE itself. Thus the test results achieved using a single plane are identical to testing using dual plane.

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 three site audits as reported in CC-20-0132791 *[CR_0132791]*, and two site audits as reported in CC-21-0351632 *[CR_0351632]* and CC-22-0448219 *[CR_0448219]*.

No sites have been visited as part of this evaluation.

2.8   Evaluated Configuration

The TOE is defined uniquely by its name and version number HUAWEI eSight 20.1.0.

2.9   Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an 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 eSight 20.1.0, 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 eSight 20.1.0 - Security Target, Version 2.1, 17 March 2022 *[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:

ICT	Information and Communication Technology
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
O&M	Operations and Maintenance
OSS	Operations Support System
PP	Protection Profile
TOE	Target of Evaluation

TÜVRheinland®
Precisely Right.

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
[CR_0132791]	Certification Report Huawei iMaster NCE V100R019C10, NSCIB-CC-0132791-CR, Version 1.0, 28 September 2020
[CR_0351632]	Certification Report Huawei iMaster NCE V100R020C10 for NCE-Fabric, NCE- FabricInsight, NCE-CampusInsight, NCE-WAN Version V100R20C10SPC100 and iMaster NCE V300R020C10 for NCE-Campus Version V300R020C10SPC100, NSCIB-CC-0351632-CR, Version 1.0, 20 September 2021
[CR_0448219]	Certification Report Huawei BSBC 2.0, NSCIB-CC-0448219-CR, Version 1.0, 25 February 2022
[ETR]	Evaluation Technical Report "Huawei eSight 20.1.0" – EAL4+, 21-RPT-1222, Version 4.0, 22 March 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	CC HUAWEI eSight 20.1.0 - Security Target, Version 2.1, 17 March 2022

(This is the end of this report.)