TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

Huawei OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300

Sponsor and developer:	**Huawei Technologies Co., Ltd.** **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-0351849-CR**
Report version:	**1**
Project number:	**0351849**
Author(s):	**Andy Brown**
Date:	**13 December 2021**
Number of pages:	**12**
Number of appendices:	**0**

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

TÜVRheinland®
Precisely Right.

CONTENTS

TÜVRheinland®
Precisely Right.

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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300. The developer of the Huawei OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300 is Huawei Technologies Co., Ltd. located in Shenzhen, 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 part of the OSN Series software which runs on the OSN Series device. The TOE consists of the Unified Transmission Software (UTS). The UTS is responsible for managing and controlling the whole OSN Series software, communication, and security features in OSN Series devices. The TOE, together with the non-TOE firmware, is packed into a software package which the user downloads along with guidance documents for correct installation of the certified configuration.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 13 December 2021 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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300, 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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300 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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei OptiX OSN 9800 V100R020C10	V100R020C10SPC300
Software File	OptiX OSN 9800 U32E_V100R020C10SPC300.zip OptiX OSN 9800 U64E_V100R020C10SPC300.zip OptiX OSN 9800 M24_V100R020C10SPC300.zip OptiX OSN 9800 M12_V100R020C10SPC300.zip OptiX OSN 9800 M05_V100R020C10SPC300.zip	V100R020C10
Software Signature File	OptiX OSN 9800 U64E_V100R020C10SPC300.zip.asc OptiX OSN 9800 U32E_V100R020C10SPC300.zip.asc OptiX OSN 9800 M24_V100R020C10SPC300.zip.asc OptiX OSN 9800 M12_V100R020C10SPC300.zip.asc OptiX OSN 9800 M05_V100R020C10SPC300.zip.asc	V100R020C10

To ensure secure usage a set of guidance documents is provided, together with the Huawei OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

To counter the security threats listed in the [ST], the TOE provides the following security features:

- Identification and authentication of administrative users
  - o Users are identified by a username and authenticated by password piror to accessing services of the TOE. The TOE is accessed via CLI (console and SSH). The TOE provides local authentication and remote authentication via RADIUS.

- Authorization
  - o The TOE maintains mutiple user groups. There are in total 4 user roles (listing from the least privileges to the most privileges): Monitor, Operator, Maintenance, and Administrator. Only authenticated users can execute commands of the TOE.

- Auditing
  - o The TOE generates audit records for security-relevant management actions. All audit records contain not only the information on the event itself but also a timestamp and – if applicable – additional information like user ID, source IP, etc. Audit records are writing to local flash storage. The TSF deletes the oldest log files if the audit trail exceeds the size of the storage device.

- Communication security
  - o The TOE provides communication security by implementing the TLS protocol. To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, TLS 1.2 and TLS 1.3 are provided with the following cipher suites:
  - o TLS1.2:
    - ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
    - ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
  - TLS1.3:
        - TLS_CHACHA20_POLY1305_SHA256 as defined in RFC8439
        - TLS_AES_256_GCM_SHA384 as defined in RFC8446
        - TLS_AES_128_CCM_8_SHA256 as defined in RFC8446
        - TLS_AES_128_GCM_SHA256 as defined in RFC8446
        - TLS_AES_128_CCM_SHA256 as defined in RFC8446
  - The TOE also provides an SFTP client for secure file downloading and uploading. Users can use the SFTP client for fault collection, log uploading, and uploading and downloading of a file and a database etc. SFTP provides:
        - Authentication of client by password or RSA public key;
        - AES encryption algorithms;
        - HMAC integrity verification algorithms;
        - Secure cryptographic key exchange using diffie-hellman-group14-sha1.

- Management traffic flow control

  - For administration of the TOE, network packages have to be sent to the TOE from the management network. When a network packet reaches the TOE from the management network, the TOE applies an information flow security policy in the form of Access Control Lists (ACLs) to the traffic before processing it. Network packets on Layer 3 from the management network arriving at a network interface of the TOE are checked to ensure that they conform to the configured packet filter policy.

- The TOE provides the following management functionalities:

  - Management of user accounts and user attributes, including user credentials;
  - Management of authentication failure policy;
  - Access control management, including the association of users and corresponding privileged functionalities;
  - Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces;
  - Management of ACLs and ACL attributes and parameters like IP addresses or address ranges;
  - Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP;
  - Management of the TOE's time;
  - All security management functions (i.e. commands related to security management) require sufficient user level for execution.

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 is part of the OSN Series software which contains Unified Transmission Software (UTS) and for the System Control and Communication. It provides the core control and management services of the device.

The non-TOE SW components include system and service attribute management, service schedule and protect, optical Layer protocol, service warning and performance, service control and monitor, and OS (Operation System).

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:
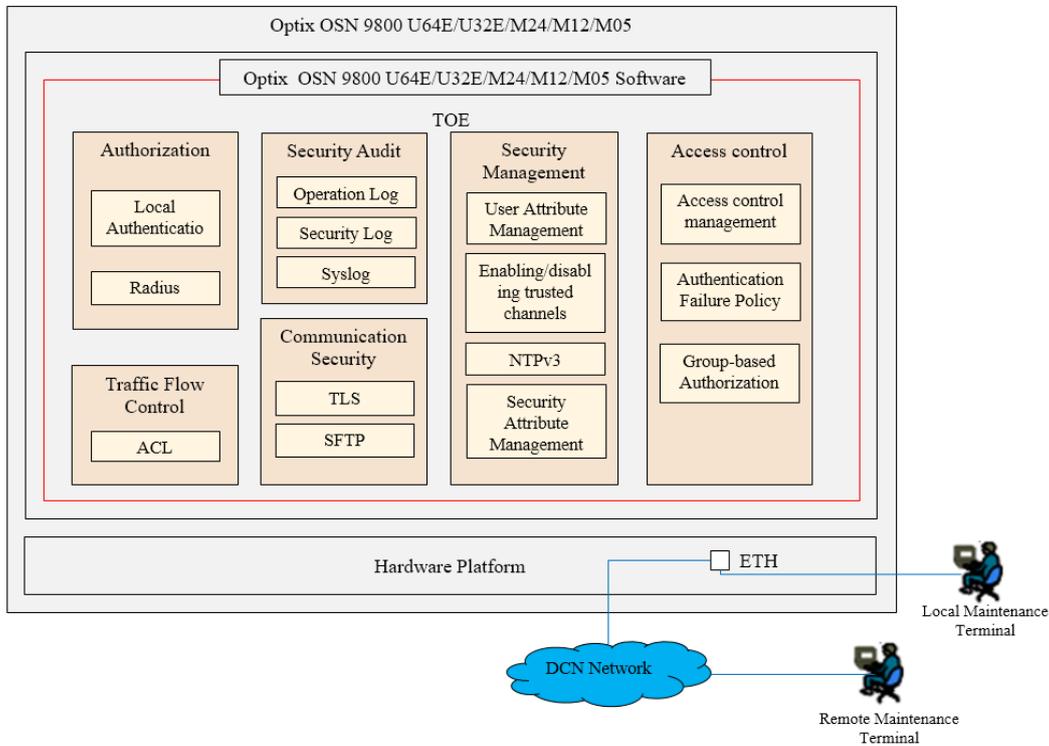
The UTS is responsible for managing and controlling the whole OSN 9800 software, communication, and security features in OSN 9800. The UTS relies on the underlying OS. The OS is responsible for processes scheduling management, file system management, memory management, IPC module (Inter Process communication), and drivers etc. The security features of the TOE are all provided by the UTS.

2.5 Documentation

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

Identifier	Version
OptiX OSN Intelligent Optical Transport Platform 9800 V100R020C10 Product Description	issue 02
Huawei OptiX OSN 9800 V100R020C10 Software - AGD_OPE	V1.1
Huawei OptiX OSN 9800 V100R020C10 Software - AGD_PRE	V1.1
Huawei OptiX OSN 9800 V100R020C10 Software - ADV_C&R	V1.0

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 focused on functional testing and manually tested all of the defined test cases. The developer grouped the 26 executed test cases into the following logical security functions:

- Auditing
- Authorization
- Authentication
- Communication security
- Security Management
- Time
- Interface

Each defined test case ran independently. There was no sequence dependency between test cases. The developer tested all the TSFIs. However, the developer focused more on the management interfaces (CLI and GUI) than the protocol interfaces (RADIUS, NTP, etc.).

The developer executed their test plan on an OSN 9800 series models U64E, U32E, M24, M12, and M05 chassis with control board TNG3CXP running V100R020C10SPC300.

The evaluator repeated 6 of the developer's test cases. In addition, the evaluator devised 10 independent evaluator tests to further complement the coverage.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- Focused analysis
  - o An analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information.
- SFR analysis
  - o The evaluator applies their knowledge of attacks applicable to the TOE type.
- Public domain analysis
  - o The evaluator performs a public domain vulnerability search for TOE specific items (TOE name, TOE-type, secure libraries, etc.)
- Network scanning tools
  - o The evaluator runs vulnerability-scanning tools to identify potential vulnerabilities.

The evaluator devised 7 penetration tests to verify that the TOE, in its operational environment, met the assurance requirements. The total test effort expended by the evaluators was 1 week. During that test campaign, 100% of the total time was spent logical tests.

2.6.3 Test configuration

The test configuration was identical to that described in section 2.6.1.

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 3 Site Technical Audit Reuse reports.

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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300.

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 OptiX OSN 9800 V100R020C10 Software Management Component V100R020C10SPC300, to be **CC Part 2 extended, 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.

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 Huawei OptiX OSN 9800 V100R020C10 Software Management Component Security Target, Issue 1.6, 02 December 2021 *[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:

ACL	Access Control List
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security CEM Common Methodology for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line interface
GUI	Graphical User Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	IT Security Evaluation Facility
IPC	Inter Process Communication
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
NTP	Network Time Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TOE	Target of Evaluation
UTS	Unified Transmission Software

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
[ETR]	Huawei OptiX OSN 9800 series software management component V100R020C10SPC300 – Evaluation Technical Report EAL4+, 21-RPT-375, Version 5.0, 13 December 2021
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Huawei OptiX OSN 9800 V100R020C10 Software Management Component Security Target, Issue 1.6, 02 December 2021

(This is the end of this report.)