Certification Report

Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
Administration Building, Headquarters of Huawei
Technologies Co., Ltd., Bantian, Longgang District,
Shenzhen, 518129, Peoples Republic of China

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

Report number:	**NSCIB-CC-2200024-01-CR**
Report version:	**1**
Project number:	NSCIB-2200024-01
Author(s):	**Andy Brown**
Date:	**27 November 2023**
Number of pages:	**11**
Number of appendices:	**0**

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

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 OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300. The developer of the Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300 is Huawei Technologies Co., Ltd. located in Shenzhen, Peoples 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 the OSN Series software which runs on the OSN Series devices. The TSF of the TOE is 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 has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 27 November 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 OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300, 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&OSN1800 V100R021C10 Software, version V100R021C10SPC300 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 OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300 from Huawei Technologies Co., Ltd. located in Shenzhen, Peoples Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software	V100R021C10SPC300

To ensure secure usage a set of guidance documents is provided, together with the Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

- Identification and authentication of administrative users
  - The TOE can authenticate administrative users by user name and password. The TOE provides a local authentication mode, or can optionally enforce authentication decisions obtained from a Radius server in the IT environment.
- Authorization
  - Authorization indicates that devices assign operation authorities to accounts according to their validity.
- Auditing
  - Logs record routine maintenance events of the TOE. Administrators can find security vulnerabilities and risks by checking logs.
- Communication security
  - The TOE provides communication security by implementing the TLS protocol and the SFTP protocol for different use cases. For the secure communication between the TOE and the EMS the TLS protocol is used. TLS1.2 and TLS1.3 are implemented.
- Management traffic flow control
  - For administration of the TOE, network packages have to be sent to the TOE from the management network. The TOE provides Access Control List (ACL) for filtering incoming information flows to management interfaces.
- Security functionality management:
  - The TOE provides security management functionalities to manage authentication, access level, managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

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]*.

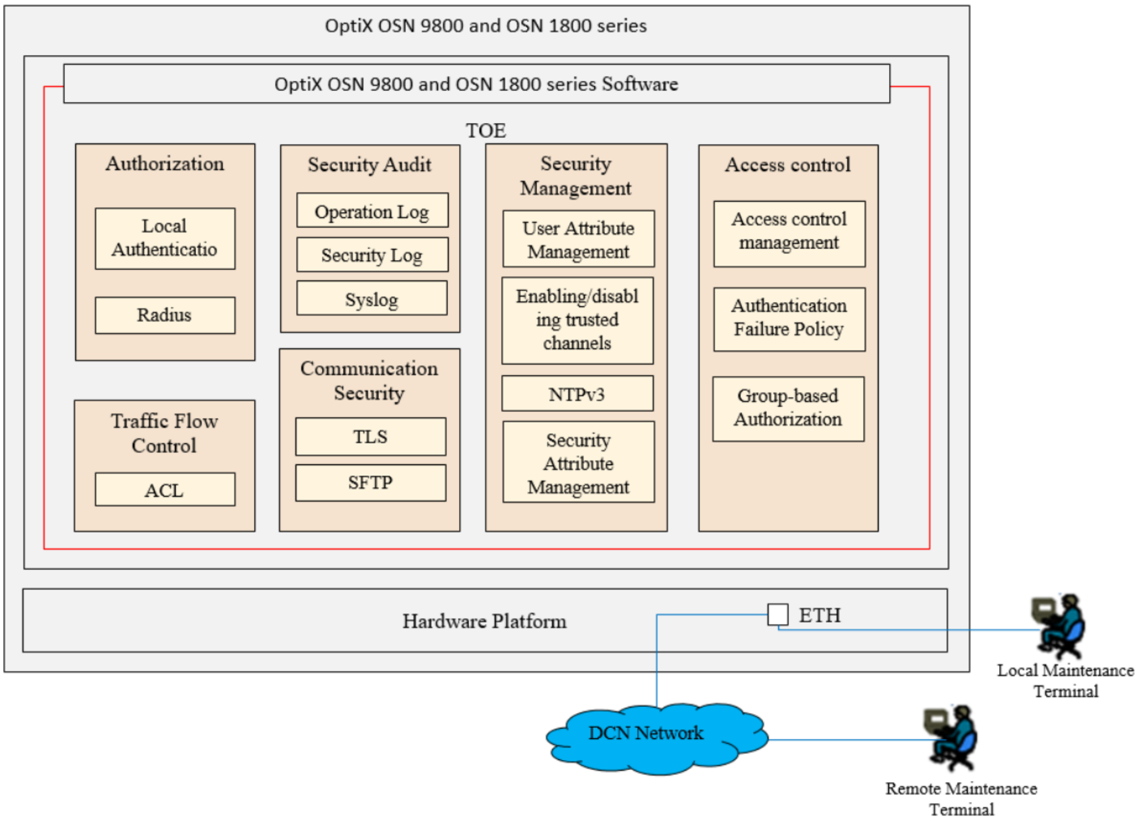
2.3.2 Clarification of scope

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 the OSN Series software which contains Unified Transmission Software (UTS) and the System Control and Communication of the OSN 9800 and OSN 1800 series of transmission devices.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:


OptiX OSN 9800 and OSN 1800 series
OptiX OSN 9800 and OSN 1800 series Software
TOE
Authorization
Local Authenticatio
Radius
Security Audit
Operation Log
Security Log
Syslog
Security Management
User Attribute Management
Enabling/disabling trusted channels
NTPv3
Security Attribute Management
Access control
Access control management
Authentication Failure Policy
Group-based Authorization
Traffic Flow Control
ACL
Communication Security
TLS
SFTP
Hardware Platform
ETH
Local Maintenance Terminal
DCN Network
Remote Maintenance Terminal

The UTS is responsible for managing and controlling the whole OSN 9800 and OSN1800 software, communication, and security features in the OSN 9800 and OSN 1800. 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
Huawei OptiX OSN9800&OSN1800 V100R021C10 Software – AGD-PRE	1.3
Huawei OptiX OSN9800&OSN1800 V100R021C10 Software -AGD_OPE	1.1
OptiX OSN 1800_V100R021C10_04_en_BEL04187	Issue 04
OptiX OSN9800_V100R021C10_04_en_31180CBG	Issue 04

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 executed test cases into the following logical security functions:

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

The evaluators analysis of the testing concluded that all TSFI were covered.

The evaluator repeated 7 of the developer's test cases.

The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or 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 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.

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 configurations for testing were identical to that described in section 2.6.1. The TOE was tested on a configuration of both the OSN 1800 and the OSN 9800 routers. The evaluators demonstrated that these TOEs represented all TOE configurations through an equivalency argumentation.

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 is no reuse of evaluation results in this certification

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. Two additional 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&OSN1800 V100R021C10 Software, version V100R021C10SPC300.

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 Report(s) for the site(s) *[STAR]* [2].

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the Huawei OptiX OSN 9800&OSN1800 V100R021C10 Software, version V100R021C10SPC300 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

[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 Huawei OptiX OSN9800&OSN1800 V100R021C10 Software Security Target, Issue 1.4, 11 September 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:

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

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 OSN 9800 and 1800 software V100R021C10SPC300” – EAL4+, 23-RPT-726, Version 1.0, 14 September 2023

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] Huawei OptiX OSN9800&OSN1800 V100R021C10 Software Security Target, Issue 1.4, 11 September 2023

[STAR-WHN] Site Technical Audit Report - Huawei Wuhan A7 Development Site, 23-RPT-669, Version 2.0, 30 August 2023

[STAR-CHG] Site Technical Audit Report - Huawei Chengdu U2 Development Site, 23-RPT-670, Version 2.0, 01 September 2023

(This is the end of this report.)