Reference: 2019-7-INF-4068- v1
Target: Pública
Date: 22.09.2023

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-7**
TOE	**Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**

References

[EXT-4679] Certification Request

[EXT-8368] Evaluation Technical Report

Certification report of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230, as requested in [EXT-4679] dated 01/02/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8368] received on 13/03/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230.

The TOE is server service software that is deployed on CloudOS, which serves as a united network controller (UNC).

UNC authenticates mobile subscribers onto the network system and tracks active and idle subscribers on the network system. UNC pages mobile subscribers when it is triggered by new data arriving for an idle subscriber at the assigned Serving GW (gateway). When a subscriber attaches to an eNodeB, the eNodeB select a UNC. UNC in turn selects the Serving GW and the PDN GW that will handle bearer packets of the subscriber. There are procedures to relocate a subscriber to a new UNC (and potentially a new Serving GW), when an active or idle subscriber moves to a new area outside of the current UNC control.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL4 + ALC_FLR.1.

Evaluation end date: 03/04/2023

Expiration Date[1]: 21/06/2028

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + ALC_FLR.1, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The UNC is a unified service node used in General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Long-Term Evolution (LTE) and 5G NSA networks. The UNC provides the functions of the serving GPRS support node (SGSN) and mobility management entity (MME) and can be used as a separate SGSN, separate MME, or combined SGSN/MME. The UNC can also be used as a single network element (NE) to manage other UNCs. The TOE is connected to WebLMT through TLS and to U2020 server through SSH.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.1 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENTS
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_FLR.1
	ALC_LCD.1
	ALC_TAT.1
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.3
FAU_STG.1
FAU_STG.3
FDP_ACC.1
FDP_ACF.1
FIA_UID.2
FIA_UAU.2
FIA_UAU.4
FIA_AFL.1
FIA_ATD.1
FIA_SOS.1
FMT_SMF.1
FMT_SMR.1
FMT_MOF.1
FMT_MSA.1
FMT_MSA.3
FMT_SAE.1
FTA_MCS.1/WebLMT
FTA_MCS.1/U2020
FTA_SSL.3
FTP_TRP.1
FTP_ITC.1

IDENTIFICATION

Product: Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230

Security Target: Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Security Target, version 2.3 (03rd March 2023).

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL4 + ALC_FLR.1.

SECURITY POLICIES

The use of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.2 ("OSP").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230, although the agents implementing attacks have the attack potential according to the Enhanced-Basic of EAL4 + ALC_FLR.1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 ("Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("Security Objectives for the Operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE provides the following security features:

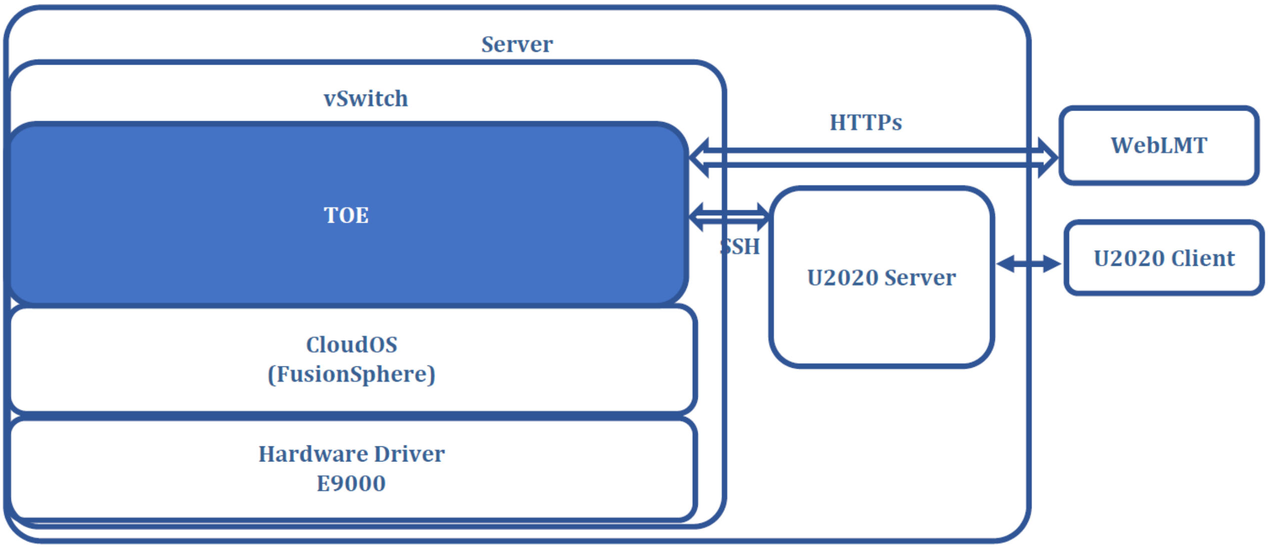
- Auditing
    - The TOE records operations on and events that occur to the device. The recorded operations and events are log messages. Log messages provide evidence for diagnosing and maintaining the TOE.
    - The log records user operations, user management, security policy configuration, system management, etc. associating the identity of the user with the event.
    - Only authorized users can view logs and users can select the log based on the time range and security level.
    - The oldest log files are deleted if the audit trail exceeds the size of store device.
- Communication security
    - The TOE supports trusted communications using TLS for the communication channel between the TOE and the WebLMT.
    - The TOE supports trusted communications using SSH for the communication channel between the TOE and the U2020 server.
- Authentication
    - The TOE supports password-based user authentication
    - The TOE can grant different privileges to the user according to user roles.
    - The TOE can enforce user password policy.
    - In order to protect the TOE, the TSF can restrict the maximum number of concurrent sessions and can lock an interactive session after a time interval. The user should re-authentication prior to unlocking the session.
    - The TOE can lock the user account for 5 minutes, if this user has 3 unsuccessful authentication attempts within 5 minutes.
- Access control
    - The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE to prevent internal traffic overload and service interruption.
    - The TOE can limit the session establishment via SSH/TLS by blacklist/whitelist filtering, which compares the client of session establishment request with specified blacklist/whitelist. The TOE can reject the session establishment from the IP address in the blacklist, while accept the session establishment request from the IP address or in the whitelist.
- Secure Management
    - The security management function of the TOE supports user management, , TLS and SSH configuration and ACL management.

PHYSICAL ARCHITECTURE

The TOE physical scope comprises both the software packages detailed in the table below and the documents described in the next section.

Software and Documents	Description	File Type	SHA256
UNCOption3_V100R001C20SPC200_Install.zip	Base software package (In the form of binary compressed files).	Software	7e9ca6d8bf906aca0bb0fe8827dc6ce0f32fd04d511474331c320a6870b289c2
UNCOption3_V100R001C20SPC200_Install.zip.asc	Signature file of base software package	Signature file	769f3b177c22a85cb48ac344ec815ad5c8a09dbda61a77b321faa664da8f34cf
UNCOption3_V100R001C20SPH230.zip	Patch software package	Software	5bffdc88c3490ef62d9ced087d9ae2317b5dcff8e4ab8873b626679a9938f246
UNCOption3_V100R001C20SPH230.zip.asc	Signature file of patch software package	Signature file	4f662935bd589ae3e76a9620c292aac0eb05099e15e9217e8e9656cd15fb5538

The figure below shows the TOE and its operational environment:



DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

Document title	Description	File Type	SHA256
Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Security Management Guide V2.0.pdf	The guidance documents of TOE	Document	2c406c21141736a91f056f1a8424ac15f9f332cb6a387feb5fa58699d4cdd249
Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Installation Guide V2.1.pdf		Document	44a3000c97b450cf6944aac1524993d10fc842c2325ab04a42c9db8daea8b4b7
Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 MML Commands Guide, part 1.pdf		Document	ed2e21d13549c895c35155827a76a3b16e12919037764fdc210a1cb68c5fad7b
UNC V100R001C20SPC200 Upgrade Guide 01 (FusionSphere+E9000 Based on WebLMT, Applicable to V100R001C10SPC300 and Later).doc	TOE base version full installation guide (for Huawei engineer only)	Document	4d96af50b72b5d91d6214313af9a50615fd89acd8bd0513a8d1337e057833b37
UNC V100R001C20SPH230 Upgrade Guide (Upgrade by Using the WebLMT) 01.doc	TOE patch version full installation guide (for Huawei engineer only)	Document	04c9450e10d6c62cfb5d00c6b6333224c6ede6a899dc52baae2f57478b9f16f3

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the evaluator premises. In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests. Within these activities, all aspects of the security architecture, which were not covered by functional testing, have been considered.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced-Basic has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in DOCUMENTS section are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230 it is necessary the disposition of the following software components:

Item	Item Type	Requirements
TOE	TOE	Huawei UNC version V100R001C20SPC200 with Patch V100R001C20SPH230
Browser	Microsoft Internet Explorer Firefox Google Chrome	Microsoft Internet Explorer 11 Firefox 64.X Google Chrome 55.X
Cloud OS	Fusion Sphere	Version HUAWEI Cloud Stack NFVI 6.5.1
vSwitch	Virtual switch	N/A
Server	E9000	Version: E9000 Chassis V100R001C10SPC522 RAM: 1113GB Hard disk: 6482GB
U2020 Server	U2020 Server	Version U2020 V300R019C10SPC540

EVALUATION RESULTS

The product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230 has been evaluated against the Security Target Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Security Target, version 2.3 (03rd March 2023).

All the assurance components required by the evaluation level EAL4 + ALC_FLR.1 have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.1, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE and the cumulative update in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the Security Target.
- The fulfillment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei UNC V001R001C20SPC200 with Patch V100R001C20SPH230, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Security Target, version 2.3 (03rd March 2023).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Huawei UNC V100R001C20SPC200 with Patch V100R001C20SPH230 Security Target, version 2.3 (03rd March 2023).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.