Reference: 2019-34-INF-3639- v1
Target: Pública
Date: 03.11.2021

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-34**
TOE	**Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-5299] Certification Request

[EXT-7069] Evaluation Technical Report

Certification report of the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270, as requested in [EXT-5299] dated 13/09/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7069] received on 26/07/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270.

The TOE is the core part of the software that is deployed into a LTE eNodeB base station, which is the wireless access node in LTE/SAE system. It provides the communication with the EPC/Backhaul network (through S1 and X2 interfaces), the management interfaces and other security related functionality.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN).

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

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4+ (ALC_FLR.1).

Evaluation end date: 01/10/2021.

Expiration Date[1]: 04/11/2026.

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 v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270, a positive resolution is proposed.

TOE SUMMARY

Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270 is the base station in LTE radio networks. The TOE is the core part of the software that is deployed into a Huawei 3900 series LTE

[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.

eNodeB base station and the major security features implemented and included in the evaluation scope are:

- Management network.
  - Identification and Authentication.
  - Access control.
  - Communications security.
- Telecom network: S1 and X2 backhaul interface protection.
- Resource management: session establishment mechanisms and VLAN separation.
- Security function management: command groups, trusted channels, users, etc.
- Digital signature: for the verification of software packages when loaded.
- Auditing of security events.

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, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
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/Local
FDP_ACF.1/Local
FDP_ACC.1/Domain
FDP_ACF.1/Domain
FDP_ACC.1/EMSCOMM
FDP_ACF.1/EMSCOMM
FIA_AFL.1
FIA_ATD.1
FIA_UAU.1/Local
FIA_UAU.2/EMSCOMM
FIA_UAU.5
FIA_UID.1/Local
FIA_UID.2/EMSCOMM
FIA_SOS.1
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.1
FTA_TSE.1/SEP
FTA_TSE.1/Local
FCS_COP.1/TLS
FCS_CKM.1/TLS

FCS_COP.1/IPsec
FCS_CKM.1/IPsec
FCS_COP.1/Sign
FTP_ITC.1

IDENTIFICATION

Product: Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270

Security Target: CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target version 1.6 (15 July 2021).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4 + ALC_FLR.1.

SECURITY POLICIES

The use of the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.3 (Organizational policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.4 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.2 (Threats) do not suppose a risk for the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270, 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.

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 detailed in [ST], chapter 4.2 (Security Objectives for the Operational Environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is pure software and it is divided in three main subsystems:

- Control.
- Baseband
- Transport.

The TOE main security functionalities are:

A. Identification and Authentication (Management network)

B. Access control (Management network)

C. Management interfaces protection (Management network)

D. Backhaul Interface protection (telecom network)

E. Resource management

F. Security function management

G. Digital signature

H. Auditing

PHYSICAL ARCHITECTURE

The TOE is a software package which includes all the TOE components and it is delivered in a single compressed file.

DOCUMENTS

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

DOCUMENT	FORMAT
Security Management Guide of Huawei 3900 Series LTE eNodeB Core Software V0.9	DOC
Installation Guide of Huawei 3900 Series LTE eNodeB Core Software V2.4	DOC
BTS3900&BTS5900 V100R015C10SPC270 MML Command Reference v1.3	ZIP
BTS3900&BTS5900 V100R015C10SPC270 Error codes V0.2	XLSX

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, verifying that the obtained results are consistent with the results obtained by the developer.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270 it is necessary the disposition of the following software components:

The TOE is the core part of the software that is deployed into a Huawei 3900 series LTE eNodeB base station and the version under evaluation is V100R015C10SPC270.

The TOE can be deployed with different physical configurations with no changes in the functionality, or in the installation procedures to be followed. The configuration used during the evaluation has been the DBS3900 LTE (Distributed base station).

The elements forming the TOE operational environment are detailed below:

- LTE eNodeB HW elements, including BBU (Baseband Unit) subrack and RRU/AAU (Remote Radio Unit / Active Antenna Unit).
- LTE eNodeB Operating System: RTOS V200R007C00.

- U2020 server providing access to the management functions of the TOE via SSL/TLS. U2020 version must be iManager U2020 V300R19C00.
- S-GW: Serving Gateway, Within the EPC the S-GW is responsible for tunnelling user plane traffic between the eNB and the PDN-GW. To do this its role includes acting as the mobility anchor point for the User Plane during handovers between eNB as well as data buffering when traffic arrives for a mobile in the LTE Idle sta
- A Public Key Infrastructure (PKI) which is a set of policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

EVALUATION RESULTS

The product Huawei 3900 Series LTE eNodeB Core Software V100R015C10SPC270 has been evaluated against the Security Target CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target version 1.6 (15 July 2021).

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 v3.1 R5 and the CEM v3.1 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 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.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DEKRA Testing and Certification S.A.U., a positive resolution is proposed.

- It must be noted that the interface between the base station and the user terminal is out of the scope of the evaluation, so the confidentiality and the integrity of the information exchanged between these elements have not been evaluated.

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] CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target version 1.6 (15 July 2021).

SECURITY TARGET

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

- CC HUAWEI LTE eNodeB Core Software V100R015C10SPC270 Security Target version 1.6 (15 July 2021).

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 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.