REF: 2015-6-INF-2036 v3	Creado: CERT10
Difusión: Expediente	Revisado: CALIDAD
Fecha: 29.09.2017	Aprobado: TECNICO

CERTIFICATION REPORT

Expediente: 2015-6

Huawei 3900 Series LTE eNodeB Software V100R011C10SPC112T

Datos del solicitante: HUAWEI Technologies Co., Ltd.

References:

[EXT-2723] Certification request of Huawei 3900 Series LTE eNodeB Software V100R011C10SPC112T

[EXT-3478] Evaluation Technical Report of Huawei 3900 Series LTE eNodeB Software V100R011C10SPC112T.

The product documentation referenced in the above documents.

Certification report of the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T, as requested in [EXT-2723] dated 13-03-2015, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3478] received on 07-07-2017.

https://oc.ccn.cni.es
Email: certificación.ccn@cni.es

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T.

The TOE is the software that is deployed into a LTE eNodeB base station, which is the wireless access node in LTE/SAE system.

Developer/manufacturer: HUAWEI Technologies Co., Ltd.
Sponsor: HUAWEI Technologies Co., Ltd.
Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
ITSEF:Epoche & Espri S.L.U..
Protection Profile: None.
Evaluation Level: Common Criteria v3.1 Release 4. EAL4 augmented with ALC_FLR.1.
Evaluation end date: 07-07-2017.
All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, as defined by the Common Criteria version 3.1 Release 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 Release 4.

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T, a positive resolution is proposed.

TOE SUMMARY

The TOE is the software that is deployed into a LTE eNodeB base station, which is the wireless access node in LTE/SAE system.
The TOE can be widely used to support the broadband wireless access of home and enterprise users. Besides, it is used to support mobile broadband access. In Huawei LTE solution, the TOE adopts a star topology, in which the transmission equipment is directly connected to the BS through FE or GE ports. The TOE networking supports various access modes, including the FE, GE, optical fibber, x digital subscriber line (xDSL), passive optical network (PON), microwave access, and satellite.
The TOE possesses the following features:

1. On an all-IP platform, thus supporting smooth upgrade;
2. Industry-leading technologies, delivering excellent performance; Easy maintenance; Flexible networking.

The major security features implemented by the TOE and subject to evaluation are:

- Identification and Authentication (Management network).
- Access control (Management network).
- Management Interfaces protection (Management network).
- UU Interface protection (radio network).
- Backhaul Interface protection (telecom network).
- Resource management.
- Security function management.
- Digital signature.
- Auditing.

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 version 3.1 Release 4.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Crriteria version 3.1 Release 4:

TOE Security Functional Requirements	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FCS_COP.1/Sign	Cryptographic operation
FCS_COP.1/SSL	Cryptographic operation
FCS_COP.1/UU	Cryptographic operation
FCS_COP.1/IPsec	Cryptographic operation
FCS_CKM.1/SSL	Cryptographic key generation
FCS_CKM.1/UU	Cryptographic key generation
FCS_CKM.1/IPsec	Cryptographic key generation
FDP_ACC.1/Local	Subset access control/Local
FDP_ACF.1/Local	Security attribute based access control/Local
FDP_ACC.1/Domain	Subset access control/Domain
FDP_ACF.1/Domain	Security attribute based access control/Domain
FDP_ACC.1/EMSCOMM	Subset access control/EMSCOMM
FDP_ACF.1/EMSCOMM	Security attribute based access control/ EMSCOMM
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1/Local	Timing of authentication/Local
FIA_UAU.2/EMSCOMM	User authentication before any action/EMSCOMM
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1/Local	Timing of identification/Local
FIA_UID.2/EMSCOMM	User identification before any action/EMSCOMM
FIA_SOS.1	Verification of secrets
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTA_TSE.1/SEP	TOE session establishment/SEP
FTA_TSE.1/Local	TOE session establishment/Local
FTP_ITC.1/IntegratedPort	Inter-TSF trusted channel

IDENTIFICATION

Product: Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) versión V100R011C10SPC112T
Security Target: Security Target of Huawei 3900 Series LTE eNodeB Software version 0.24. 2017-06-20.
Protection Profile: None.
Evaluation Level: Common Criteria version 3.1 Release 4. EAL4 + ALC_FLR.1.

SECURITY POLICIES

The use of the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T 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. In short, it establishes the need of implementing organisational policies related to the following aspects.

- **P1.Audit**: providing audit functionality.
- **P2. RoleManagement**: providing different people access.
- **P3.UU_Secure channel**: encypting/decrypting the data exchanged over the UU interface.

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.

- **A.PhysicalProtection**: TOE protection against unauthorized physical access.
- **A.TrustworthyUsers:** measures in place to establish trust into and train users of the TOE.
- **A.NetworkSegregation:** separation between management network, the telecom network and the signal network.
- **A.TrustNetwork:** telecom network between security gateway and EPC(S-GW/MME) is secure and trusted
- **A.Support:** reliable time stamps for the generation of audit records
- **A.SecurePKI:** There exists a well managed protected public key infrastructure.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) vV100R011C10SPC112T, although the agents implementing attacks have the attack potential according to the enhanced basic attack potential 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 categorized below.

- **T1.InTransitConfiguration**: violation of the BS file confidentiality or integrity while transferring
- **T2. InTransitSoftware**: violation of the BS software/patches confidentiality or integrity while transferring
- **T3.UnauthenticatedAccess**: disclose or modification of the configuration data stored in the TOE.
- **T4.UnwantedNetworkTraffic_M**: Unwanted network traffic sent to the TOE from management network.
- **T5.UnwantedNetworkTraffic_T**: Unwanted network traffic sent to the TOE from telecommunication network.
- **T6. UserTraffic**: gain unauthorized knowledge about the user.
- **T7.UnauthorizedAccess**: gain access to commands or information he is not authorized for.

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 categorized below.

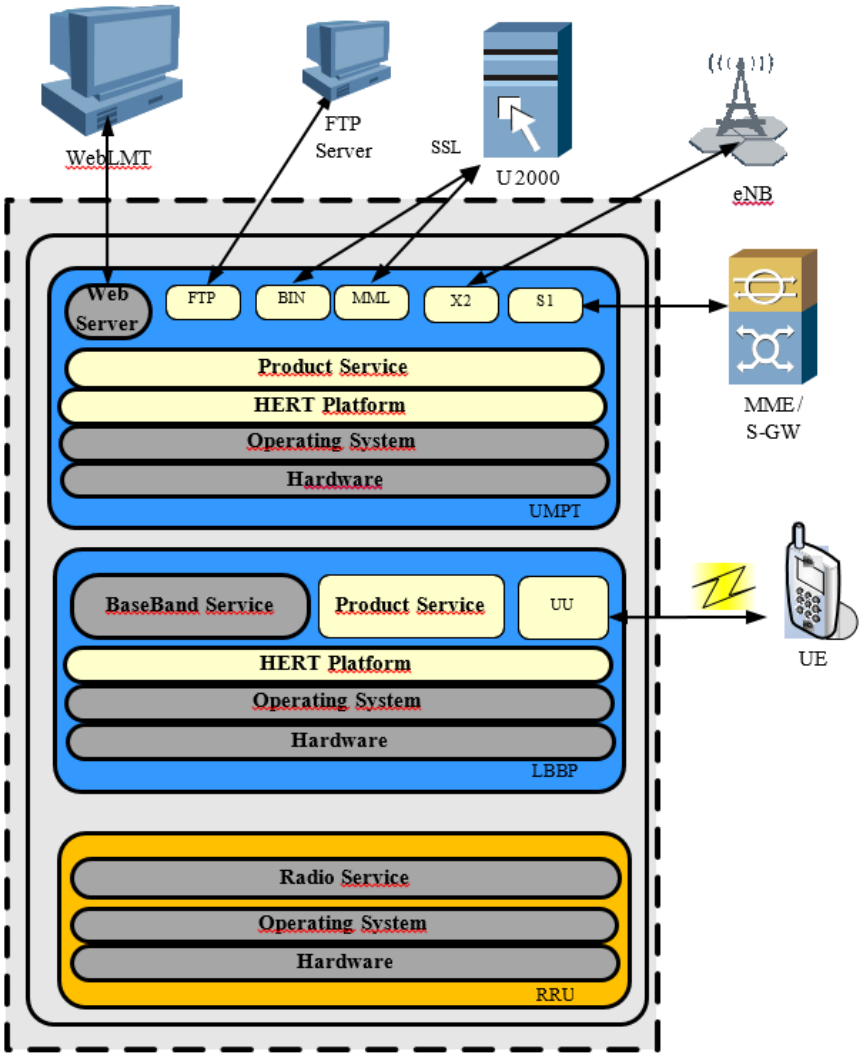
- **OE. PhysicalProtection**: protection against unauthorized physical access.
- **OE.TrustworthyUsers**: trustworthness and training of the users.
- **OE.NetworkSegregation**: assessmentt of the separation of management, telecom and signal networks.
- **OE. TrustNetwork**: the telecom network between security gateway and EPC(S-GW/MME) is trusted and secure
- **OE.Support**: providing reliable time stamps for the generation of audit records.
- **OE. SecurePKI**: the certificates used by the TOE and its client are managed by the PKI.

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 following figure includes the TOE Logical Scope, where all the connections to the TOE are indicated, and also the way the TOE is deployed in the different boards of the product:



PHYSICAL ARCHITECTURE

TOE is composed of software and documents.

Software and Documents	Description	Remark
Software.csp	Board software package (In the form of binary compressed files)	The software packages which are the TOE will be digitally signed to ensure their legitimacy and integrity.
Firmware.csp	BootROM package (In the form of binary compressed files)	

Software and Documents	Description	Remark
The install guide, commissioning and maintenance documents of eNodeB	Including the documents listed in the following table (*).	The guidance documents of LTE eNodeB Software

(*) List of documents considered as guidance:

Document
Security Management Guide of Huawei 3900 series LTE eNodeB Software, v0.6, Jun 2017
Installation Guide of Huawei 3900 Series LTE eNodeB (AGD_PRE) v0.7, Jun 2017
ADV_FSP Functional Specification of Huawei 3900 Series LTE eNodeB Software V0.46, Jun 2017
macro_en.ini, November 2016

DOCUMENTS

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

- Security Management Guide of Huawei 3900 series LTE eNodeB Software, v0.6, Jun 2017.
- Installation Guide of Huawei 3900 Series LTE eNodeB (AGD_PRE) v0.7, Jun 2017.
- ADV_FSP Functional Specification of Huawei 3900 Series LTE eNodeB Software V0.46, Jun 2017.
- macro_en.ini, November 2016.

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

The evaluator has defined and performed the penetration tests taking into account the security requirements defined in the security target, and the external interfaces defined in the functional specification.

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version number:

- Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T

To have the TOE in its expected secure configuration in accordance with the security target, the steps described in section *5 Secure Configuration* of the preparative user guidance must be followed. A batch configuration file is provided to ease the TOE configuration.

EVALUATION RESULTS

The product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T has been evaluated against the Security Target: Security Target of Huawei 3900 Series LTE eNodeB Software version 0.24. 2017-06-20.

All the assurance components required by the evaluation level EAL4 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4, as defined by the Common Criteria v3.1 Release 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 Release 4.

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.
- Before deletion of a Domain user, the security administrator must be sure that the Domain user has been forced to logout.
- If the password policy is going to be changed, the security administrator has to be sure that old users update its password according to the new policy.
- [FSP046] provides an access control table specifying the BIN and MML commands available to each user group. According to the assumption A.TrustworthyUsers described in [ST024], each user will be trusted commensurate with their privileges. As the privileges of a user are given by its access group, it is assumed that each user will behave correctly in the use of its allowed commands. It should be noted that, for example, a user from the group G_1 (role USER), has enough rights to disable some security features of the TOE, moving the TOE to an unsecured state (e.g. SET FTPSCLT, SET SSLAUTHMODE,…). This problem is covered with the assumption A.TrustworthyUsers which supposes highly qualified and trustworthy TOE users.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Software (a.k.a. eNodeB) version V100R011C10SPC112T, a positive resolution is proposed.
The certifier strongly recommends to the TOE consumer:

- to strictly follow the steps indicated in the installation documentation.

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, Release 4 September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Release 4 September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Release 4 September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 4 September 2012.

[FSP046] ADV_FSP Functional Specification of Huawei 3900 Series LTE eNodeB Software V0.46, Jun 2017.

[ST024] Security Target of Huawei 3900 Series LTE eNodeB Software version 0.24. 2017-06-20

[CCDB-2006-04-004] STsanitising for publication. CCMC, April 2006.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Security Target of Huawei 3900 Series LTE eNodeB Software version 0.24. 2017-06-20.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Security Target of Huawei 3900 Series LTE eNodeB Software version 0.25. 2017-09-14.