REF: 2014-45-INF-1417 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 14.01.2015	Approved by: TECNICO

CERTIFICATION REPORT

File: 2014-45 Huawei LTE V100R008C01SPC820

Applicant: 440301192203821 HUAWEI Technologies Co., Ltd.

References:

[EXT-2646] Certification request of Huawei LTE V100R008C01SPC820

[EXT-2648] Evaluation Technical Report of Huawei LTE V100R008C01SPC820.

The product documentation referenced in the above documents.

Certification report of the product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820, as requested in [EXT-2646] dated 19-11-2014, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-2648] received on 9/12/2014.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820.

The TOE is a Software component of Huawei 3900 series LTE eNodeB implementing a complete access control and session establishment mechanisms to avoid unauthorised entities from accessing the TOE resources. Audit functionality is also provided.

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: No.

Evaluation Level: Common Criteria v3.1 R4 - EAL4+ (ALC_FLR.1).

Evaluation end date: 5/12/2014.

All the assurance components required by the evaluation level EAL4+ (augmented with ALC_FLR.1 Basic flaw remediation) 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 + ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820, a positive resolution is proposed.

TOE SUMMARY

The TOE is a Software component of Huawei 3900 series LTE eNodeB implementing a complete access control and session establishment mechanisms to avoid unauthorised entities from accessing the TOE resources. Audit functionality is also provided.

The TOE can be widely used to support the access control and events records for the product used for the broadband wireless access of home and enterprise users and to support mobile broadband access.

The major security features implemented by the TOE and subject to evaluation (no assurance can be supposed to any other functionality) to are:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

1. **Identification and Authentication**
2. **Access control**
3. **Auditing**
4. **Resource management**
5. **Security function management**

This security features are detailed in section “1.4.2 TOE major security features” of [ST].

Figure 1 shows the position of the TOE (eNobeB AC deployed in eNB) in a LTE/SAE network.

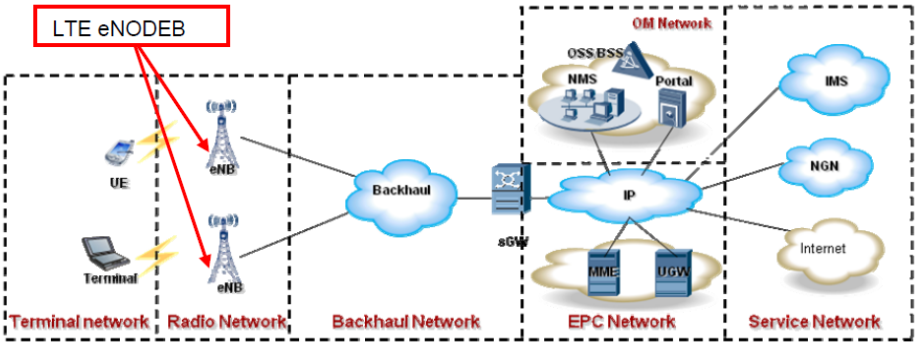

Figure 1

The TOE is a Software component of Huawei 3900 series LTE eNodeB implementing a complete access control and session establishment mechanisms to avoid unauthorised entities from accessing the TOE resources. Audit functionality is also provided. No assurance can be assigned to any other functionality of the TOE or product and, although it is a network device, security on the network interfaces has not been evaluated.

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 Basic flaw remediation, according to Common Criteria v3.1 R4.

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	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 the Common Criteria v3.1 R4:

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
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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TOE Security Functional Requirements	Description
FMT_SMR.1	Security roles
FTA_TSE.1/SEP	TOE session establishment/SEP
FTA_TSE.1/Local	TOE session establishment/Local

IDENTIFICATION

Product: Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820.

Security Target: Security Target of Huawei 3900 Series LTE eNodeB Access Control Software, v3.0 24th November 2014.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 - EAL4+ (ALC_FLR.1).

SECURITY POLICIES

The use of the product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820 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.

Policy 01: P1.Audit

The TOE shall provide audit functionality:

- Generation of audit information.
- Storage of audit log.
- Review of audit records.

Policy 02: P2.Authorisation

The TOE shall implement a complete access control and session establishment mechanisms to avoid unauthorised entities from accessing the TOE resources.

Policy 03: P3. Resources

The TOE shall implement VLAN separation and IP based ACLs to avoid resource overhead.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

Assumption 01: A.TrustedNetworks

It is assumed that the **management network** (integrated port & FTP interfaces) is secure and **trusted**.

It is assumed that the **telecom network** (S1 and X2 interfaces) is secure and **trusted**.

It is assumed that **signal network** (UU interface) is secure and **trusted**.

It is assumed that **management network, the telecom network and the signal network** are **separated** between each other.

Assumption 02: A.PhysicalProtection

It is assumed that the TOE is protected against unauthorized physical access.

Assumption 03: A.TrustworthyUsers

It is assumed that the organization responsible for the TOE and its operational environment has measures in place to establish trust into and train users of the TOE commensurate with the extent of authorization that these users are given on the TOE. (For example, super users and users that are assigned similar privileges are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them.)

Assumption 03: A.Support

The operational environment must provide the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records

THREATS

The TOE Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820 is defined in [ST] where all the security objectives are derived from assumptions and OSPs only, and therefore, in the security problem the statement of threats is not present.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

Environment objective 01: OE.TrustedNetworks

The TOE operational environment shall implement IT and Non-IT measures guaranteeing that the management network (integrated port & FTP interfaces) is secure and trusted.

The TOE operational environment shall implement IT and Non-IT measures guaranteeing that the telecom network (S1 and X2 interfaces) is secure and trusted.

The TOE operational environment shall implement IT and Non-IT measures guaranteeing that signal network (UU interface) is secure and trusted.

The TOE operational environment shall guarantee that management network, the telecom network and the signal network are separated between each other.

Environment objective 02: OE.PhysicalProtection

The TOE (i.e., the complete system including attached interfaces) shall be protected against unauthorized physical access.

Environment objective 03: OE.TrustworthyUsers

Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

Environment objective 04: OE.Support

Those responsible for the operation of the TOE and its operational environment must ensure that the operational environment provides the following supporting mechanisms to the TOE: Reliable time stamps for the generation of audit records.

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

From the Logical point of view, 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

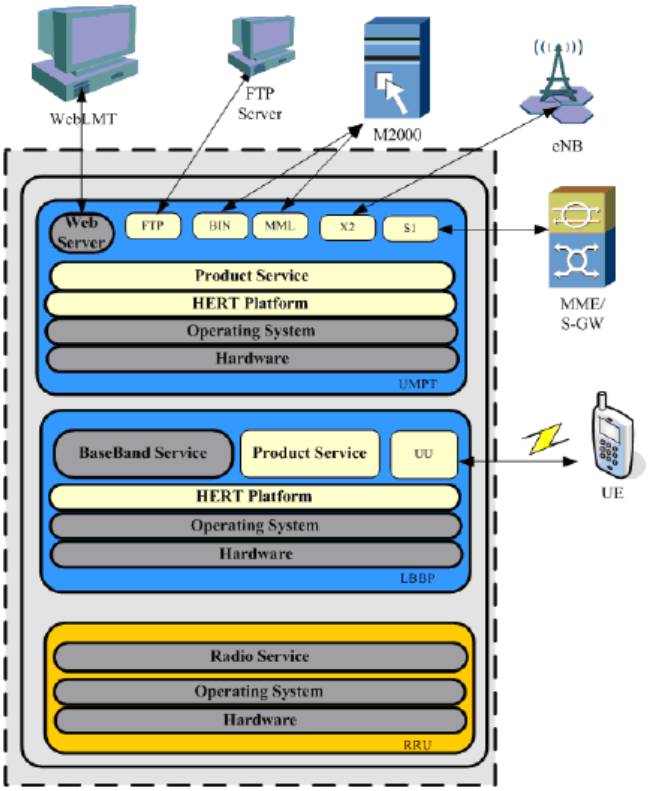

Figure 2

The TOE is pure software. OS and other software provided by particular products is TOE environment. In the above diagrams, the content of the blue areas (excluding the grey boxes) are parts of the TOE (although not all the functionality belongs to the TSF as mentioned later). The TOE includes Product Service and HERT platform. The security functionality of the TOE includes the implementation of a complete access control mechanism, a session establishment control mechanism and events recording functionality.

The TOE security functionality, as described in detail in the section 1.4 TOE Overview of [ST] is:

- Identification and Authentication.
- Access control.
- Auditing.
- Resource management.
- Security functionality management.

For each of the identified parts of the TOE, a correspondence between them and the TOE security functionality can be achieved. That way, for each part, the appropriate security associated functionality is indicated a table in section 1.5.1 Logical Scope of [ST].

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

PHYSICAL ARCHITECTURE

The release packages for the TOE are composed of software and documents. The TOE Software packages are in the form of binary compressed files.

The TOE software packages can be downloaded and stored in the UMPT board, and then, they will be checked up, unpacked, and then distributed to each board module.

The list of the files and documents required for the TOE are the following, both the software and documents are available on the sponsor's support website.

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 (OUT OF SCOPE OF THE EVALUATION).
FIRMWARE.CSP	BOOTROM PACKAGE (IN THE FORM OF BINARY COMPRESSED FILES)	
TOE INSTALL GUIDE, COMMISSIONING AND MAINTENANCE DOCUMENTS	INCLUDING THE DOCUMENTS LISTED IN THE FOLLOWING SECTION	INCLUDING THE DOCUMENTS LISTED IN THE FOLLOWING TABLE

DOCUMENTS

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

- Undocumented MML Description (HERT-BBU) v0.1, July 2014
- Undocumented MML Description (LTE) v0.1, July 2014
- Hert BBU MML reference for LTE v 0.1, April 2014
- Security Management Guide of Huawei 3900 series LTE eNodeB Software, v 1.0, July 2014
- Installation Guide of Huawei 3900 Series LTE eNodeB (AGD_PRE) v1.5, July 2014
- BTS3900 V100R008C01SPC820 (eNodeB) Parameter Reference v1.0 (July 2014)
- BTS3900 V100R008C01 (eNodeB) MML Command Reference v1.1
- Functional Specification of Huawei 3900 Series LTE eNodeB Software (ADV_FSP) v0.60, July 2014
- Functional Specification of Huawei BS Annexes v0.2 March 2014

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification, the SFRs description included in [ST], and the subsystems and modules defined in the TOE design documentation.

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals.

The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST].

The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report.

The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones.

The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in [ST].

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in [ST].

All identified vulnerabilities in the form of backdoors can be considered closed if the TOE is installed and operated according to the [ST] and related documentation.

The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. 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 measures required by the developer are applied.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EVALUATED CONFIGURATION

The TOE is defined by its name and version number:

- Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820.

To set up the TOE in a way consistent to the evaluated configuration and the operational environment defined in [ST], users must follow the steps included in the following installation and operation manuals:

- Installation Guide of Huawei 3900 Series LTE eNodeB (AGD_PRE) v1.5, July 2014.
- BTS3900 V100R008C01SPC820 (eNodeB) Parameter Reference v1.0.
- BTS3900 V100R008C01 (eNodeB) MML Command Reference v1.1.
- Hert BBU MML reference for LTE v 0.1, April 2014.
- Security Management Guide of Huawei 3900 series LTE eNodeB Software, v 1.0, July 2014.

EVALUATION RESULTS

The product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820 has been evaluated against the Security Target Security Target of Huawei 3900 Series LTE eNodeB Access Control Software, v3.0 24th November 2014.

All the assurance components required by the evaluation level EAL4 + 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 evaluation level EAL4 + ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

This section describes several important aspects that could influence the use of the product, taking into account the scope of the findings of the evaluation and its security target [ST].

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment.

The following usage recommendations are given:

1. 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

2. The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
3. Before deletion of a Domain user, the security administrator must be sure that the Domain user has been forced to logout.
4. 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.

The user is the one responsible of securitizing the networks in which the TOE operates in order to fulfill the OE.TrustedNetworks objective included in the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820, a positive resolution is proposed.

In addition to the previous evaluator recommendations for the use of the TOE, it is necessary to remark that the TOE is a Software component of Huawei 3900 series LTE eNodeB implementing an event log functionality and a complete access control and session establishment mechanisms. No assurance can be assigned to any other functionality of the TOE or the product and although it is a network device, **security on the network interfaces has not been evaluated**.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LTE	Long Term Evotution
OC	Organismo de Certificación
OE	Objective for the Environment
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ST] Security Target of Huawei 3900 Series LTE eNodeB Access Control Software, v3.0 24th November 2014.

SECURITY TARGET

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

- Security Target of Huawei 3900 Series LTE eNodeB Access Control Software, v3.0 24th November 2014.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es