REF: 2010-23-INF-808 v4	Created by: CERT3
Target: Expediente	Revised by: CALIDAD
Date: 22.12.2011	Approved by: TECNICO

CERTIFICATION REPORT

File: 2010-23 Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100

Applicant: 440301192W HUAWEI

References:

[EXT1114] Certification request of Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100

[EXT1493] Evaluation Technical Report of Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100.

The product documentation referenced in the above documents.

Certification report of the product Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100, as requested in [EXT1114] dated 21/12/2010, and evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report EXT1493 received on 16/12/2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
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 Software V100R004C00SPC100.

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.

Protection Profile: No conformance to a Protection Profile is claimed.

Evaluation Level: Common Criteria EAL3+ (ALC_CMC.4; ALC_CMS.4).

Evaluation end date: 16/12/2011.

All the assurance components required by the evaluation level EAL3 (augmented with ALC_CMC.4; ALC_CMS.4) have been assigned a “PASS” verdict. Consequently, the laboratory EPOCHE & ESPRI assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3+ (ALC_CMC.4; ALC_CMS.4), as defined by the [CC-P3] and the [CEM].

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100, a positive resolution is proposed.

TOE SUMMARY

The 3900 series LTE eNodeB 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 3900 series LTE eNodeB adopts a star topology, in which the transmission equipment is directly connected to the BS through FE or GE ports. The 3900 series LTE eNodeB 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 3900 series LTE eNodeB possesses the following features:

- Eight-antenna MIMO, increasing coverage with fewer sites;
- High integration, reducing the overall size;
- On an all-IP platform, thus supporting smooth upgrade;
- Industry-leading technologies, delivering excellent performance;
- Easy maintenance through the Web LMT; Flexible networking.

The major security features implemented by 3900 series LTE eNodeB and subject to evaluation are:

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Authentication. Operators using the WebLMT to access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.
- Access control. 3900 series LTE eNodeB implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations.
- Auditing. Audit records are created for security-relevant events related to the use of 3900 series LTE eNodeB.
- Communications security. 3900 series LTE eNodeB offers SSL/TLS channels for FTP, MML (man-machine language, which is a kind of Command Line Interface), and BIN (Huawei's private binary message protocol) access to the TOE.
- UU Interface encryption. LTE air interface support AES and SNOW 3G service data encryption, which ensures the privacy of user session.
- S1 Interface encryption. The IPSec protocol is used in the communication with the MME/S-GW.
- X2 Interface encryption. The IPSec protocol is used in the communication with other LTE eNodeBs.
- Resource management. VLAN (Virtual Local Area Network) are implemented to separate the traffic from different flow planes, which reduce traffic storms and avoid resource overhead. ACL (Access Control List) implements packet filtering features to restrict resource use via IP address, ports, etc. Those features protect the 3900 series LTE eNodeB against various unauthorized access from unauthorized NEs.
- Security function management. The TOE offers management functionality for its security functionality.
- Digital signature. In the production and distribution phases, the digital signature scheme, protect the software package by message digest and signature.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 and the evidences required by the additional components ALC_CMC.4 and ALC_CMS.4, according to [CC-P3].

Assurance Class	**Assurance Components**
Security Target	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
Development	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
Guidance	AGD_OPE.1, AGD_PRE.1
Life Cycle	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1
Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Vulnerability Analysis	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, as stated by its Security Target, and according to [CC-P2].

Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling FIA_ATD.1 User attribute definition FIA_SOS.1 Verification of secrets FIA_UID.1 Timing of identification FIA_UAU.1 Timing of authentication FIA_UAU.5 Multiple authentication mechanisms
Security Management (FMT)	FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
User Data Protection (FDP)	FDP_ACC.1/Local Subset access control FDP_ACF.1/Local Security attribute based access control FDP_ACC.1/Domain Subset access control FDP_ACF.1/ Domain Security attribute based access control FDP_ACC.1/EMSCOMM Subset access control FDP_ACF.1/EMSCOMM Security attribute based access control
Trusted path/channels (FTP)	FTP_ITC.1/ IntegratedPort Inter-TSF trusted channel FTP_TRP.1/WebLMT Trusted path
TOE Access (FTA)	FTA_TSE.1/SEP TOE session establishment FTA_TSE.1/Local TOE session establishment
Cryptographic Support (FCS)	FCS_COP.1 /Sign Cryptographic operation FCS_COP.1 /SSL Cryptographic operation FCS_COP.1 /S1 Cryptographic operation FCS_COP.1 /X2 Cryptographic operation FCS_COP.1 /UU Cryptographic operation FCS_CKM.1 /SSL Cryptographic key generation FCS_CKM.1 / S1 Cryptographic key generation FCS_CKM.1 / X2 Cryptographic key generation FCS_CKM.1 / UU Cryptographic key generation
Security Audit (FAU)	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

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

	FAU_STG.3 Action in case of possible audit data loss

IDENTIFICATION

Product: Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100

Security Target: Security Target of Huawei 3900 Series LTE eNodeB Software, v2.6; October 17th, 2011.

Protection Profile: No conformance to a Protection Profile is claimed.

Evaluation Level: CC v3.1 r3 - EAL3+ (ALC_CMC.4; ALC_CMS.4).

SECURITY POLICIES

The use of the product Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100 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. The TOE shall provide the following audit functionality:

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

P2.S1_Encryption. The TOE shall encrypt/decrypt of the data exchanged over the S1 interface.

P3.X2_Encryption. The TOE shall encrypt/decrypt of the data exchanged over the X2 interface.

P4.UU_Encryption. The TOE shall encrypt/decrypt of 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

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.

A.NetworkSegregation. It is assumed that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separated from the UU, S1 and X2 interface networks.

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

A.SecurePKI. There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100, although the agents implementing attacks have the attack potential according to the BASIC of CC-EAL3 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 threat agents can be categorized as either:

Agent	Description
Eavesdropper	An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.
Internal attacker	An unauthorized agent who is connected to the management network.
Restricted authorized user	An authorized user of the TOE who has been granted authority to access certain information and perform certain actions.

In the first and second cases, the users are assumed to be potentially hostile with a clear motivation to get access to the data. In the last case, all authorized users of the TOE are entrusted with performing certain administrative or management activities with regard to the managed device. Consequently, organizational means are expected to be in place to establish a certain amount of trust into these users.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

However, accidental or casual attempts to perform actions or access data outside of their authorization are expected. The assumed security threats are listed below.

Threats by Eavesdropper

Threat: T1. InTransitConfiguration	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BS file while transferring, violating its confidentiality or integrity.
Asset	A3. In transit configuration data
Agent	Eavesdropper

Threat: T2. InTransitSoftware	
Attack	An eavesdropper in the management network succeeds in accessing the content of the BS software/patches while transferring, violating its confidentiality or integrity.
Asset	A1.Software and patches
Agent	Eavesdropper

Threats by Internal Attacker

Threat: T3.UnwantedNetworkTraffic	
Attack	Unwanted network traffic sent to the TOE will cause the TOE's processing capacity for incoming network traffic to be consumed thus failing to process legitimate traffic. This may further causes the TOE fails to respond to system control and security management operations. The TOE will be able to recover from this kind of situations.
Asset	A4. Service
Agent	Internal Attacker

Threat: T4.UnauthenticatedAccess	
Attack	An attacker in the management network gains access to the TOE disclosing or modifying the configuration data stored in the TOE in a way that is not detected.
Asset	A2.Stored configuration data
Agent	Internal Attacker

Threats by restricted authorized user

Threat: T5.UnauthorizedAccess	
Attack	An user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
Asset	A2.Stored configuration data
Agent	Restricted authorized user

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment.

With this purpose, the security objectives declared for the TOE operational environment are the following:

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

OE.NetworkSegregation. The TOE environment shall assure that the network interfaces that allow access to the TOE's user interfaces are in a management network that is separated from the networks that the TOE serves over the UU and S1 and X2 interfaces.

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.

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.

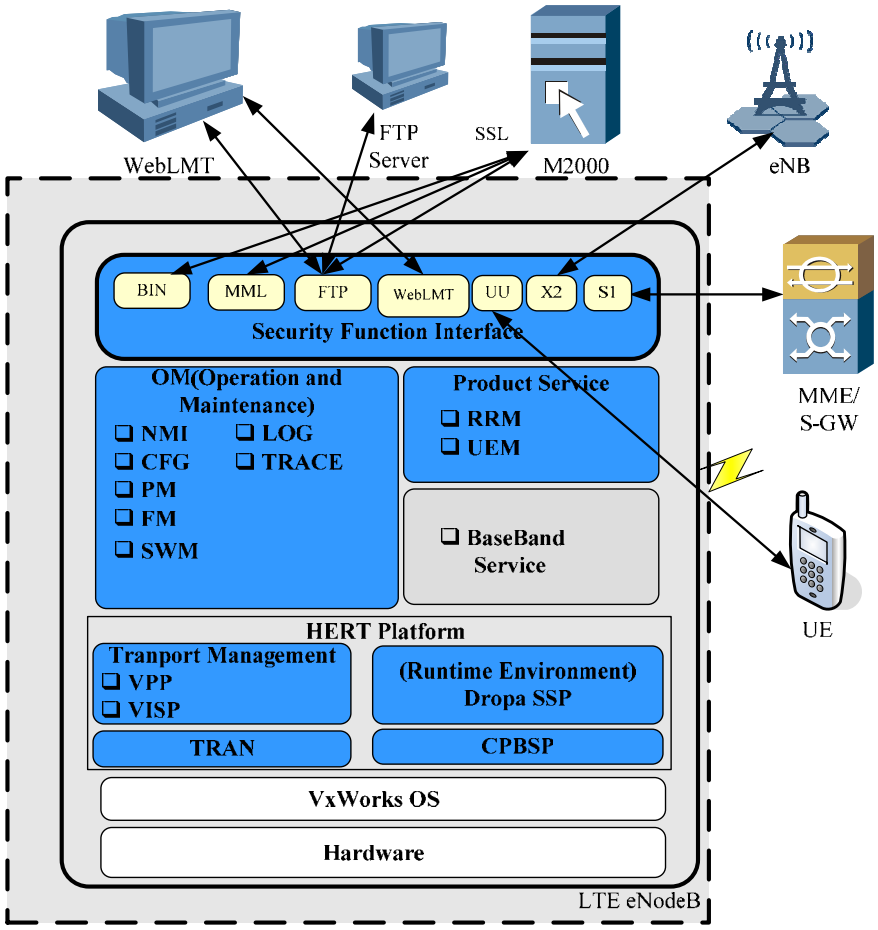
OE. SecurePKI. There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ARCHITECTURE

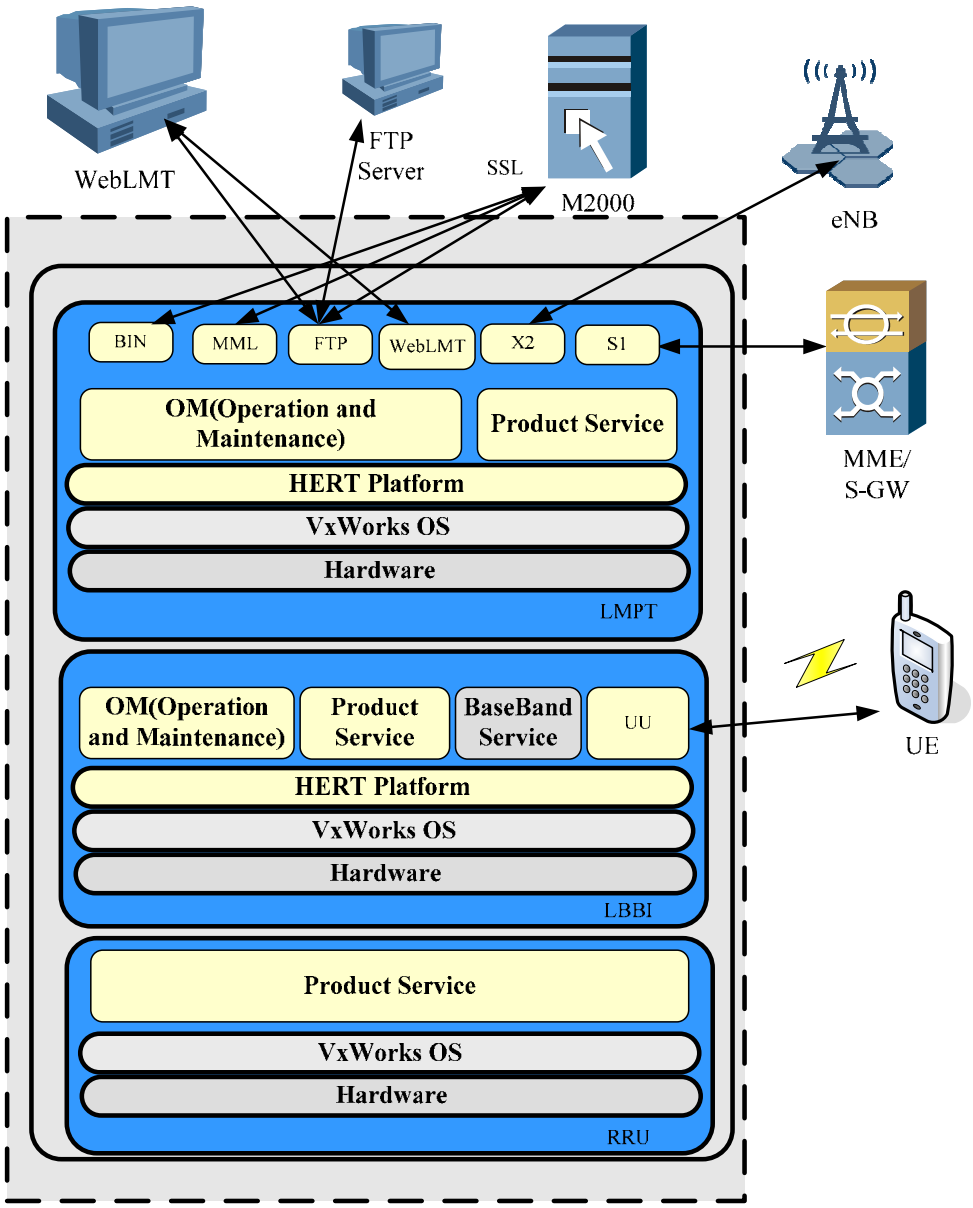
The TOE is pure software. OS and other software provided by particular products is TOE environment.

The software architecture of the TOE is indicated in the following figure:



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.



In the above diagrams, the content of the blue areas (excluding the grey boxes) are parts of the TOE. The TOE includes Operation and Maintenance (OM), Product Service, Transport Management, TRAN, CPBSP, Dopra SSP and HERT platform.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

DOCUMENTS

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

- Security Target of Huawei 3900 Series LTE eNodeB Software v2.6 Oct 2011
- Undocumented MML Description LTE v0.3 Nov 2011
- Installation Guide of Huawei 3900 Series LTE eNodeB (AGD_PRE) v0.22
- Undocumented MML Description HERT-BBU v0.1 Oct 2011
- HERT-BBU MML Command Reference V200R007
- LTE MML Command Reference V100R004C00SPC100
- Security Management Guide of Huawei 3900 Series LTE eNodeB Software v0.1
- Functional Specification of Huawei 3900 Series LTE eNodeB Software (ADV_FSP) v0.50 Nov 2011
- Functional Specification of Huawei BS Annexes v0.3 Nov 2011

PRODUCT TESTING

The evaluator, as part as the independent tests, has:

- repeated a sample of the developer tests, following his procedures in order to gain confidence in the results obtained.
- executed their own test scenarios to operate the TOE.

The main objective when repeating the developer tests is to execute enough tests to confirm the validity of their results.

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

For all the test cases, the obtained results were consistent with those obtained by the developer, obtaining in all of them a positive result.

The evaluator considers that both the TSFIs and subsystem tests defined by the developer are correct having checked that the results obtained when repeating the tests are the same than the results obtained by the developer.

Regarding the independent tests, the evaluator has designed a set of tests following a suitable strategy for the TOE type taking into account:

- increasing test coverage of each interface varying the input parameters: search for critical parameters in the TSFIs interactions, incorrect behaviour suspicion with specific input values;
- complete coverage of all the SFRs defined in the security target.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The evaluator has designed his TSFIs and subsystems independent test cases including all the external interfaces. Moreover, the evaluator has carried out tests with parameters of the TSFIs and subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed his TSFIs and subsystems independent test cases including all the security requirements defined in the security target.

The process has 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.

The TOE configuration or setup is described in each test. Evaluator devised test results are consistent with the expected results.

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.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

PENETRATION TESTING

The approach of the penetration testing focused on testing the weakest points of the TOE by design or by technologies that are commonly known to be easy to exploit.

The independent penetration testing devised attack vector and performed test cases covering the following attacks categories for this TOE: Audit, Covert channels, security mechanisms bypass, code injection, protocol attacks…

EVALUATED CONFIGURATION

The TOE is defined by its name and version number: **Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100.**

The hardware platform used to deploy the TOE is BBU3900 (environment, not evaluated).

The following components were used as environment during the evaluation:

- An M2000 server providing access to the management functions of the TOE via SSL. **M2000 version must be iManager M2000 Version 2 Release11 C01 CP1301. (Common Criteria EAL3+ALC_CMC.4+ALC_CMS.4 evaluated version).**
- LTE eNodeB Operating System: Vxworks, version 5.5.1 (environment, not evaluated).

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EVALUATION RESULTS

The product "Huawei 3900 Series LTE eNodeB Software, version V100R004C00SPC100" has been evaluated against the "Security Target of Huawei 3900 Series LTE eNodeB Software, v.2.6"; October 17th, 2011.

All the assurance components required by the level EAL3+ (ALC_CMC.4; ALC_CMS.4) have been assigned a "PASS" verdict. Consequently, the laboratory EPOCHE & ESPRI assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3+ (ALC_CMC.4; ALC_CMS.4) methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

In this section, 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, are listed.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- The management network shall be a secure network, free of attackers.
- The fulfilment of the OE.SecurePKI must be strictly observed due to the intensive use of TLS/SSL to ensure the communications security.
- It is very important the adequate fulfilling of the installation procedures; the installation procedure may be vulnerable if those procedures are not followed.
- The operators of the product shall perfectly know the contents of all the products manuals, including the functional specification which contains the use details of the BIN interfaces and the recommended secure values.
- The functional specification provides an access control table specifying the BIN and MML commands available to each user group. According to the assumption A.TrustworthyUsers described in the security target, each user will be trusted commensurate with their privileges. As the privileges of a user are given by the above mentioned rights table, 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, DLD SOFTWARE…). Moreover, a user from the group G_20 (role GUEST), has enough rights to connect to the underlying operating system using Serial Port Operation commands. This problem is although covered with the assumption A.TrustworthyUsers which supposes highly qualified and trustworthy TOE users.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei 3900 Series LTE eNodeB Software V100R004C00SPC100, a positive resolution is proposed.

Additionally, the Certification Body recommends potential users to observe the following recommendations extracted from the TOE's user guidance:

- The TOE's consuming organizations should develop and implement a Security Policy to review and delete TOE's expired user accounts. The TOE is not able to deny access to users whose accounts have an expired password. This SFR is not declared within the TOE's Security Target.
- The TOE's consuming organizations should develop and implement a Security Policy to notify and force users to reset their user password in case changes are made in the TOE's Password Policy. The TOE is not able to notify users or enforce modifications in the user accounts if a modification in the password policy is made after a user password is created. This SFR is not declared within the TOE's Security Target.
- The TOE's consuming organizations should develop and implement a Security Policy to force OS to lock user sessions in those terminals which are left unattended while sessions are established with the TOE from the client side, or force TOE's users to disconnect the client from the TOE before leaving their terminal unattended.

This certification is recognised under the terms of the [CCRA] for components up to EAL3+ (ALC_CMC.4; ALC_CMS.4) and it is also covered by the [SOGIS], but only for components until EAL2.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
OS	Operating System
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, R3 Final, July 2009.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- [CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.
- [CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.
- [CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

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 Software, v2.6“; October 17th, 2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es