MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2010-25-INF-849 v3
Target: Público
Date: 21.03.2012

Created by: CERT3
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

File: 2010-25 Huawei WCDMA NodeB Software V200R013C01SPC010
Applicant: 440301192W HUAWEI

References:

- [EXT1116] Certification request of Huawei WCDMA NodeB Software.
- [EXT1531] Evaluation Technical Report of Huawei WCDMA NodeB Software.
- The product documentation referenced in the above documents.

Certification report of the product Huawei WCDMA NodeB Software V200R013C01SPC010, as requested in [EXT1116] dated 21-12-2010, evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report [EXT1531] received on 16/12/2011, and in compliance with [CCRA] for components up to EAL3+ (ALC_CMC.4; ALC_CMS.4) and with [SOGIS], but only for components until EAL2.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei WCDMA NodeB Software V200R013C01SPC010.

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 3.1 R3 - 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 and ALC_CMS.4) have been assigned a “PASS” verdict. Consequently, the laboratory EPOCHE & ESPRI S.L. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3+ (augmented with ALC_CMC.4 and ALC_CMS.4), as defined by the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the product Huawei WCDMA NodeB Software V200R013C01SPC010, a positive resolution is proposed.

TOE SUMMARY

Huawei WCDMA NodeB (the equipment) use the advanced wideband, multi-mode system, and modular design, and has features such as the compact size, high integration, low power consumption, and easy and quick deployment. The innovative design and flexible combinations of the function modules and auxiliary devices encourage Huawei to diversify multi-mode NodeB products.

Huawei WCDMA NodeB (the equipment) has a cutting-edge modular design, thus compatible with functional modules of different network systems. With simply three types of units, the 3900 series NodeBs feature small size, high integration, low power consumption, easy and fast deployment.

The innovative design and flexible combinations of the functional modules and auxiliary devices lead to the diversity of NodeB. The operators can install boards of different network systems in one cabinet to form a NodeB that applies to different scenarios. This accelerates the introduction of new radio network technologies and complies with the development trend of the mobile network towards integration of different network systems.

The 3900 series NodeBs are based on IP switch and multi-carrier technologies and support the bandwidth of over 100 Mbit/s. This ensures a high data transmission rate for users during mobile data service expansion. The Huawei WCDMA NodeB (the equipment) networking supports various access modes, including the FE, GE, optical fiber, microwave access, and satellite.

The major security features implemented by Huawei WCDMA NodeB Software and subject to evaluation are:

- Authentication. Operators using remote access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.
- Access control. Huawei WCDMA NodeB Software implements role-based access control for LMT and M2000. NodeB supports various kinds of users: Local users through LMT ("admin", "guest"), Domain users through LMT and "EMSCOMM" user through M2000. Depending on the kind of user and its certain privileges, a concrete user will be able to perform its applicable set of actions into the TOE.
- Auditing. Audit records are created for security-relevant events related to the use of NodeB.
- Communications security. Huawei WCDMA NodeB Software 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. 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 NodeB against various unauthorized access from unauthorized NEs. The communication between the Network Elements and NodeB uses SSL, and certificates for this purpose are deployed.
- 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. The TOE verifies the software digital signature's validity.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil EAL3+ (ALC_CMC.4; 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
Vulnerability Analysis	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the CC Part 2 [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 Inter-TSF trusted channel
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_CKM.1 /SSL 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 FAU_STG.3 Action in case of possible audit data loss

IDENTIFICATION

Product: Huawei WCDMA NodeB Software, version V200R013C01SPC010

Security Target: Huawei WCDMA NodeB Software Security Target, Version 1.19, 11.11.2011.

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 WCDMA NodeB Software V200R013C01SPC010 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.

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

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 separate from the management flows, service flows and signaling flows the application (or, public) networks that the network device hosting the TOE serves.

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 WCDMA NodeB Software, version V200R013C01SPC010, 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 in the management network 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. 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 INTERACTIVE NETWORK 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 date 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	A 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

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 management flows, signaling flows and service flows.

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

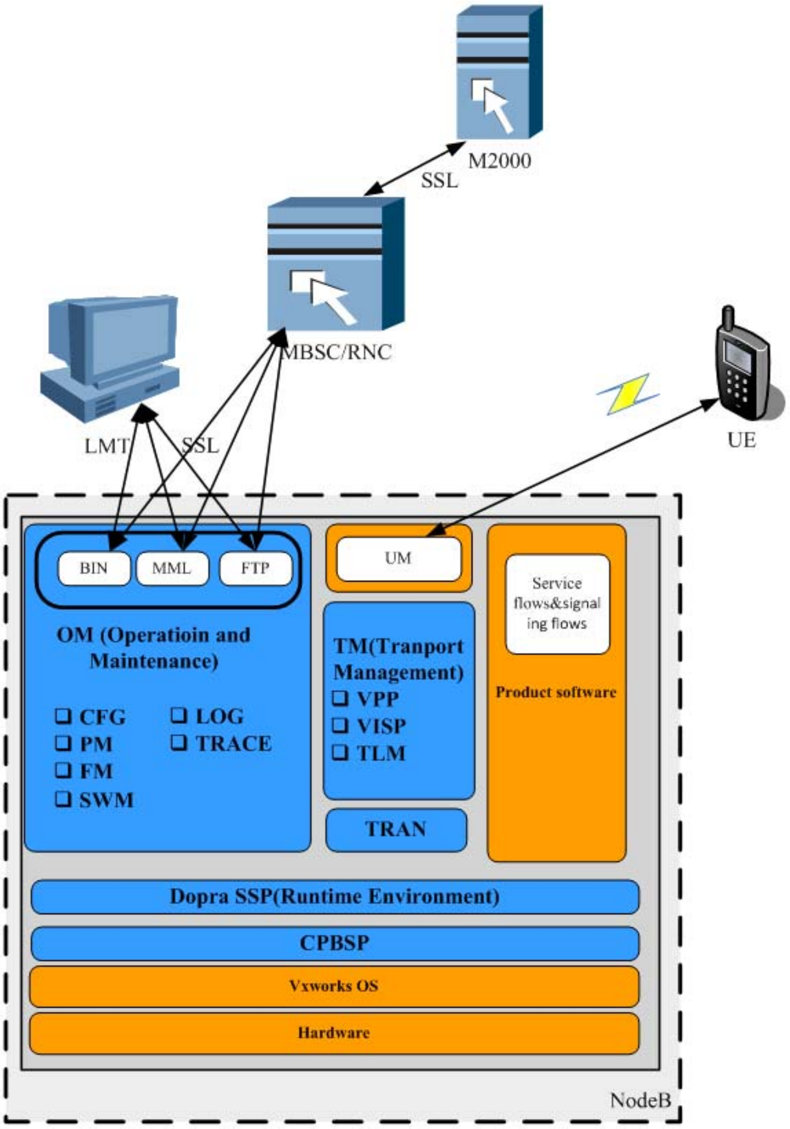
There exists a well managed protected public key infrastructure. The certificates used by the TOE and its client are managed by the PKI.

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

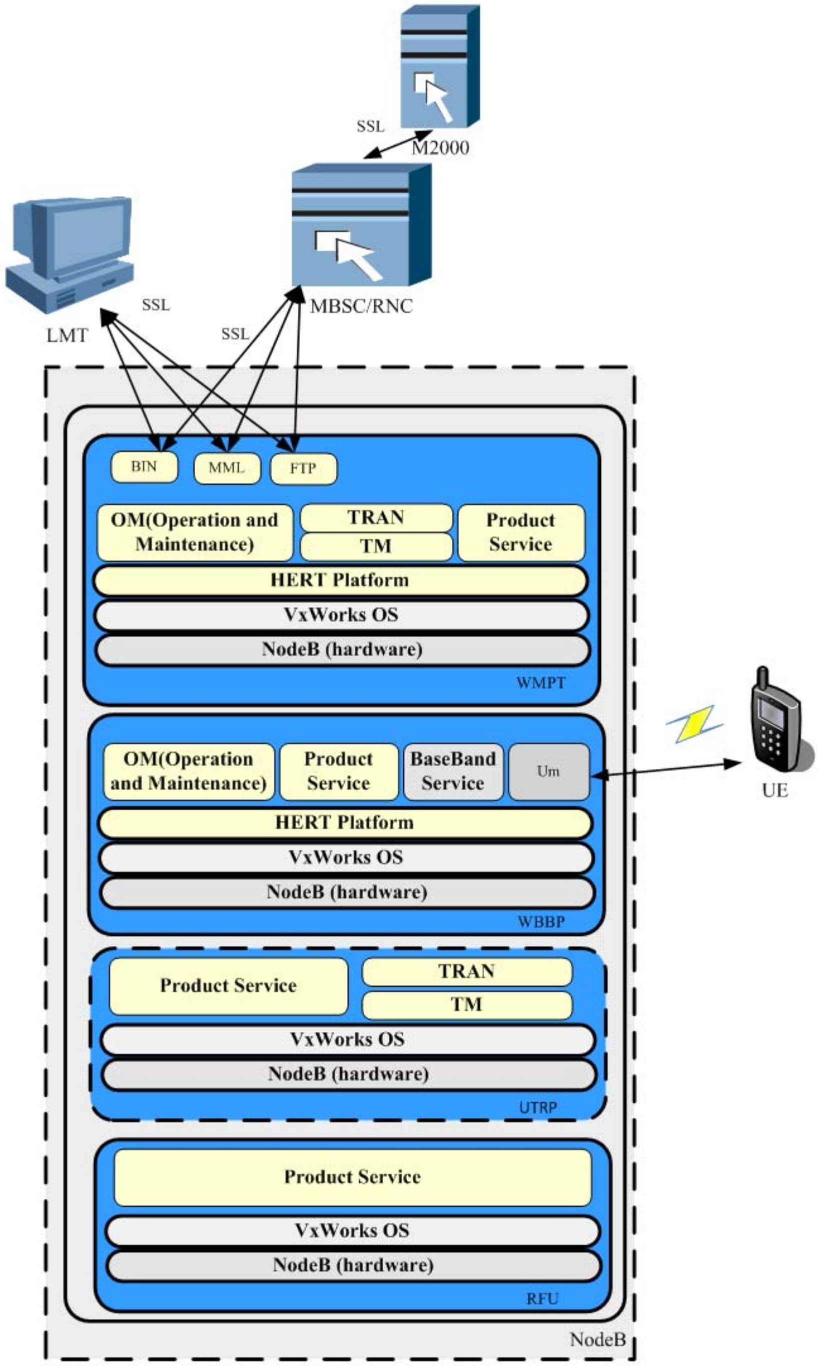
LOGICAL ARCHITECTURE

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



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

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 diagram, the blue areas are parts of the TOE. NodeB includes Operation and Maintenance (OM), Baseband Service, and HERT platform.

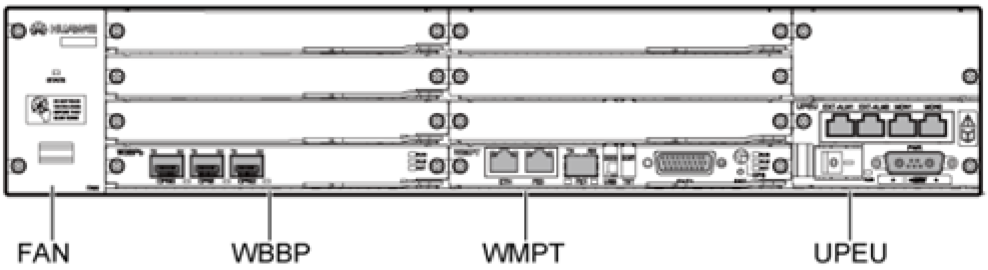
PHYSICAL ARCHITECTURE

The physical structure of Huawei WCDMA NodeB Software can be:

- DBS3900: Distributed base station. The DBS3900 typifies the compact design, easy installation, and low power consumption. In addition, it can reside in the spare space of an existing 2G site. The RRU also has a compact design and light weight. It can be installed close to the antenna to decrease feeder loss and improve system coverage. All the previously mentioned features of the distributed NodeB facilitate the site selection, network planning and optimization. This enables the operators to efficiently deploy a high-performance 3G network with a low TCO because less manpower, electric power, and space are required during network construction.
- BTS3900: Indoor cabinet macro base station. The BTS3900, as one of the most compact indoor macro NodeBs in the telecommunication industry, boasts large and expandable capacity. It is light, and supportive of the GSM-WCDMA dual-mode application.
- BTS3900A: Outdoor cabinet macro base station. The BTS3900A, one of the most compact outdoor cabinet macro NodeBs in the telecom industry, boasts light weight and easy transportation due to its stackable design.
- BTS3900L: Large indoor cabinet macro base station. This type of NodeB is just like BTS3900 but it can provide more cabinet space in order to facilitate the evolution to a multi-mode base station.

The TOE can be deployed in all these physical configurations with no changes in the functionality, or in the installation procedures to be followed.

The TOE runs into the BBU3900 subrack and in the RFU. The structure of BBU3900 is shown in the following figure:



The BBU3900 contains, at least, the following mandatory boards:

- The WCDMA Baseband Process Unit (WBBP), whose purpose is to provide an interface between BBU3900 and Radio Remote Unit (RRU) or Radio Frequency Unit (RFU)
- The WCDMA Main Processes and Transmission unit (WMPT), which is the main board of BBU3900.
- The Universal Power and Environment Interface Unit (UPEU), whose purpose is providing power to the whole BBU3900 subrack.

- The FAN unit of the BBU3900 controls the fan speed, monitors the temperature of the FAN unit, and dissipates the heat from the BBU.

In addition to these boards, another one can be added to incorporate some certain capabilities to the whole equipment, whose name is Universal Transmission Processing unit (UTRP). In this board, some TOE functionality can be deployed once connected to the equipment.

DOCUMENTS

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

- Huawei WCDMA NodeB Software Security Target v1.19, 11th November 2011
- WCDMA product manual_AGD. Draft C (2011-02-16), February 2011
- Security Parameters Recommended Values, v1.0
- NodeB MML Command Reference, v1.3
- CC Installation Guide of NodeB (AGD_PRE), v0.04
- HERT BBU MML Command Reference, v1.3
- NodeB BIN&MML Command Rights, v1.2
- Functional Specification Node B, v0.65
- Undocumented MML Description (Node B), v0.2
- HERT BBU Undocumented MML Description, v1.1
- Functional Specification of Huawei BS Annexes, v0.4

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.

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, Certificates management, Identification & Authentication bypass, Access control bypass, Denial of service, Password management, Software integrity.

EVALUATED CONFIGURATION

The TOE, that it is just software, is defined by its name and version number:

- **Huawei WCDMA NodeB Software, version V200R013C01SPC010**

But, given the physical architecture described above, two different configurations belong to the scope of the evaluation:

- A configuration where BBU3900 does not have an UTRP board connected, and where the entire TOE functionality is deployed in the WMPT, WBBP and RFU.
- A configuration where BBU3900 has an UTRP board connected, and where the TOE is deployed in WMPT, UTRP, WBBP and RFU.

EVALUATION RESULTS

The product "Huawei WCDMA NodeB Software, V200R013C01SPC010" has been evaluated against the "Huawei WCDMA NodeB Software Security Target, v1.19, 11th November 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 evaluation level EAL3+ (ALC_CMC.4; ALC_CMS.4), 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 following recommendations, regarding the secure usage of the TOE, have been collected along the evaluation process and are detailed to be considered when using the product:

- 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 use secured computers to interact with the TOE.
- 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. 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 abovementioned rights table, it is assumed that each user will behave correctly in the use of its allowed commands. This problem is although 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 WCDMA NodeB Software, version V200R013C01SPC010, a positive resolution is proposed.

Additionally, the Certification Body recommends potential users to observe the following recommendations:

- 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.

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

ACL	Access Control List
BBU	(Base Station)'s Base Band Unit
BIN	Huawei’s private binary message protocol
CC	Common Criteria
CCN	Centro Criptológico Nacional
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
FE	Physical acces
FTP	File Transfer Protocol
GE	Physical acces
LMT	Local Maintenance Terminal
MML	Man-Machine Language
NE	Network Element
OM	Operation and Maintenance
OS	Operating System
PKI	Public Key Infrastructure
RFU	Radio Frequency Unit
RRU	Radio Remote Unit
SFR	Security Function Requirement
SOGIS	Senior Officials Group for Information Systems Security
SSL/TLS	Secure Sockets Layer/Transport Layer Security
TCO	Total Cost of Ownership
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UPEU	Universal Power and Environment Interface Unit
UTRP	Universal Transmission Processing unit
VLAN	Virtual Local Area Network
WBBP	WCDMA BaseBand Process
WCDMA	Wideband Code Division Multiple Access

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.
- [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: “Huawei WCDMA NodeB Software Security Target, Version 1.19”, 11.11.2011.