REF: 2010-26-INF-859 v1	Created by: CERT3
Target: Público	Revised by: CALIDAD
Date: 30.03.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2010-26 Huawei WiMAX BS Software version V300R003C01SPC100

Applicant: 440301192W HUAWEI

References:

- [EXT1117] Certification request of Huawei WiMAX BS Software
- [EXT1549] Evaluation Technical Report of Huawei WiMAX BS Software
- The product documentation referenced in the above documents.

Certification report of the product Huawei WiMAX BS Software version V300R003C01SPC100, as requested in [EXT1117] dated 21-12-2010, and evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report [EXT1549] 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.

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 WiMAX BS Software version V300R003C01SPC100.

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; 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+ (ALC_CMC.4; 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 WiMAX BS Software version V300R003C01SPC100, a positive resolution is proposed.

TOE SUMMARY

World Interoperability for Microwave Access (WiMAX) is a next-generation IP-based wireless communication technology that can provide broadband wireless access in many scenarios, such as mobility, nomadic, portable, and mobile applications, under the non line sight circumstance. In the aspect of Specific support business, WiMAX technology, with its high bandwidth and improved quality of service (QoS) guarantees mechanisms to provide users with mobile or fixed scenarios of high-speed Internet access (HSI), high-quality Voice over IP (VoIP) service (based on NGN or IMS), video On-demand, mobile TV and other services.

The Huawei WiMAX BS Software complies with IEEE 802.16e standards. Currently, the Huawei WiMAX BS Software satisfies the application requirements of high-end mobile WiMAX networks, and thus is applicable to global markets. Its coverage and capacity are expanded through multi-antenna technologies, its maintainability and testability are improved, and thus it provides subscribers with the wireless broadband access services of large capacity and high quality.

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 WiMAX solution, the TOE adopts a star topology, in which the transmission

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

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:

- 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 M2000 and the Web LMT;
- Flexible networking.

The major security features included in the TOE and subject to evaluation are:

- Authentication. Operators using local access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords. Authenticated access through the integrated port is enforced using SSL client authentication.
- Access control. The TOE 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 the TOE.
- Communications security. The TOE 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.
- R1 Interface encryption. The TOE air interface channel uses CCM mode 128-bit AES encryption for its data transitions to prevent unauthorized access and to prevent unauthorized users to control forged control messages or to perform message replay attacks.
- R6 Interface encryption. The IPSec protocol is used in the communication with the ASN-GW.
- 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 TOE 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.

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

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3+ (ALC_CMC.4; ALC_CMS.4), according to CC Part 3 [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 its Security Target and to 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/ IntegratedPort Inter-TSF trusted channel FTP_TRP.1/WebLMT Trusted path

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

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 /R1 Cryptographic operation FCS_COP.1 /R6 Cryptographic operation FCS_CKM.1 /SSL Cryptographic key generation FCS_CKM.1 / R1 Cryptographic key generation FCS_CKM.1 / R6 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 WiMAX BS Software, version V300R003C01SPC100

Security Target: Security Target of Huawei WiMAX BS Software, v0.94, October 10th, 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 WiMAX BS Software, version V300R003C01SPC100, 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.R1_ENCRYPTION

The TOE shall encrypt/decrypt of the data exchanged over the R1 interface.

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

P3.R6_ ENCRYPTION

The TOE shall encrypt/decrypt of the data exchanged over the R6 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

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 R1 and R6 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 WiMAX BS Software, version V300R003C01SPC100, 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.

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

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. 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

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

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

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 R1 and R6 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.

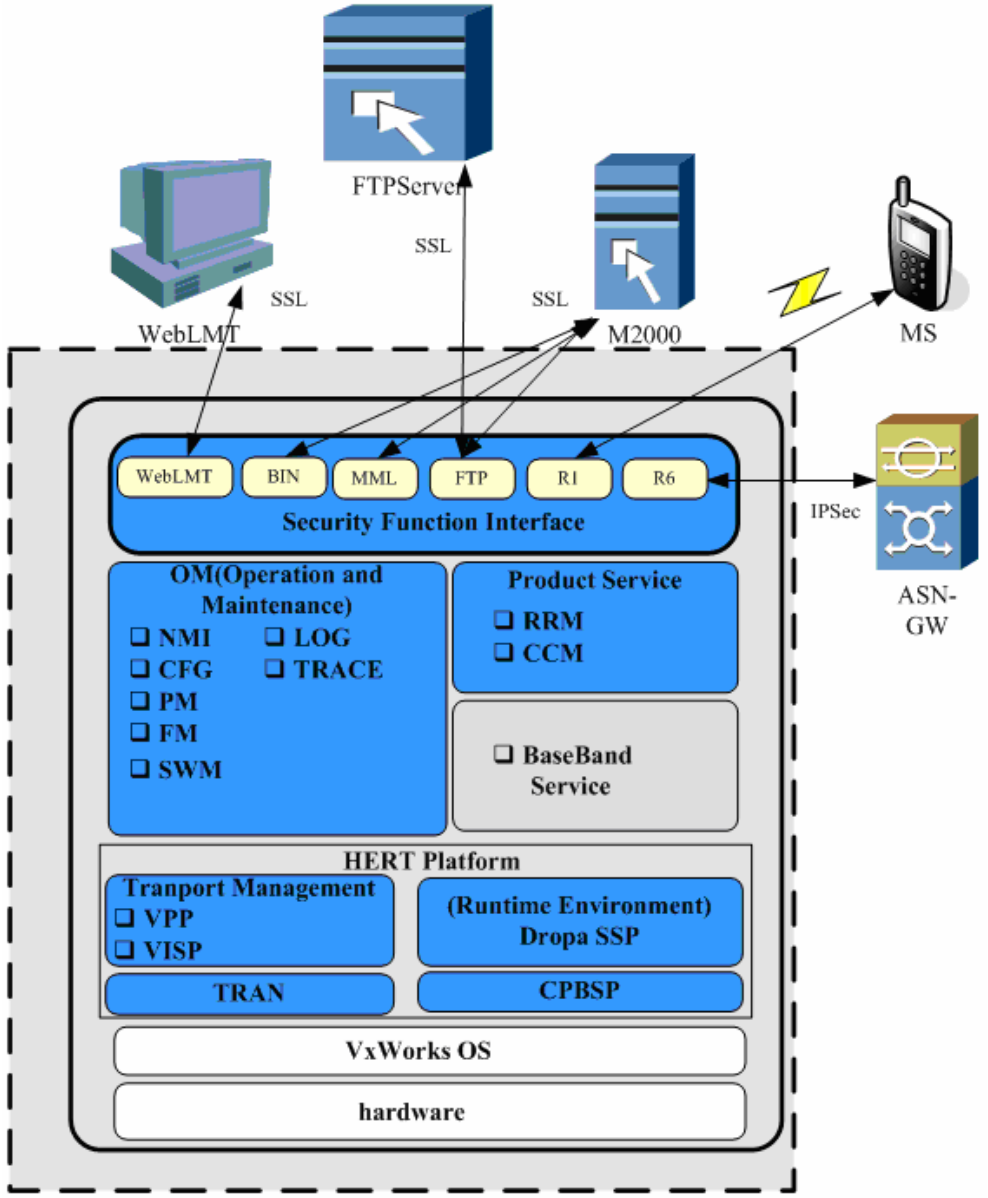
ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

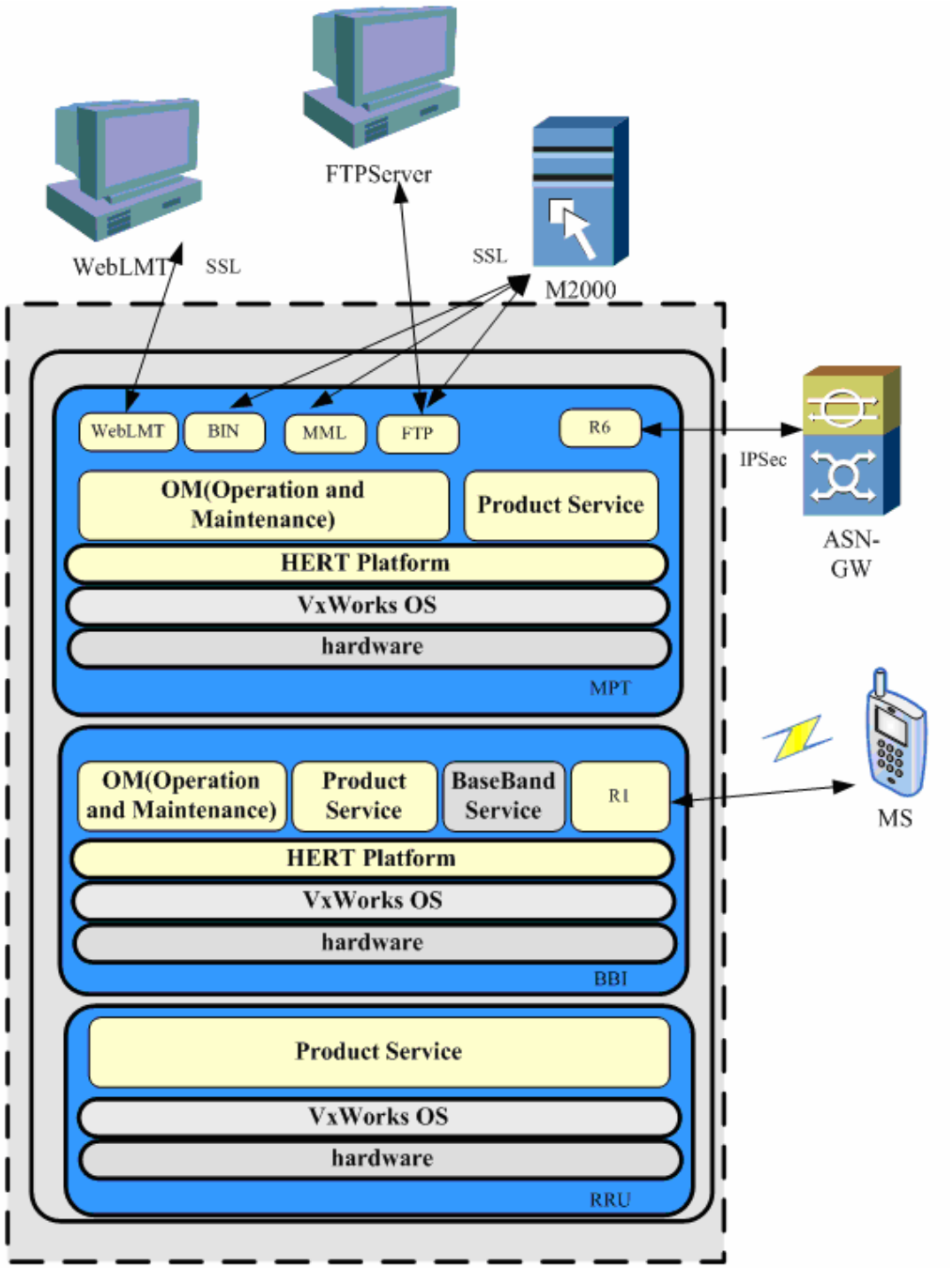
The software architecture of the TOE is indicated in the following figure:



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

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, and HERT platform.

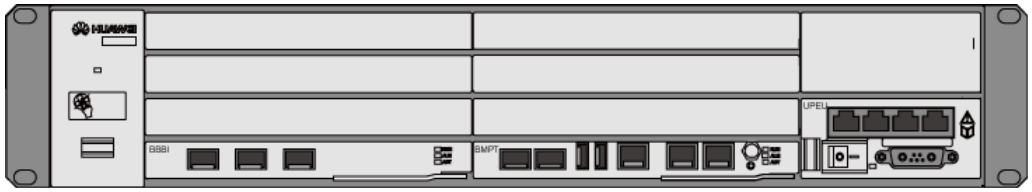
ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

PHYSICAL ARCHITECTURE

The TOE can be deployed in one of the following physical configurations with no changes in the functionality, or in the installation procedures to be followed:

- DBS3900 WiMAX: Distributed base station. The DBS3900 WIMAX is characterized by its small footprint, easy installation, and low power consumption. Therefore, the DBS3900 WIMAX can be easily installed in a spare space at an existing site. The RRU is also compact and light. It can be installed close to the antenna to reduce feeder loss and to improve system coverage.
- BTS3900 WIMAX: Indoor cabinet macro base station. The BTS3900 WIMAX is a compact indoor macro base station. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.
- BTS3900A WIMAX: Outdoor cabinet macro base station. The BTS3900A WIMAX is a compact outdoor macro base station. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.
- BTS3900L WIMAX: Large indoor cabinet macro base station. The BTS3900L WIMAX is a compact indoor macro eNodeB. It applies to the scenarios of centralized installation and replacement of traditional macro base stations.

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



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

- The BWA Baseband Processing and radio Interface Unit (BBBI), whose purpose is to provide an interface between BBU3900 and Radio Remote Unit (RRU).
- The BWA Main Processes and Transmission unit (BMPT), which is the main board of BBU3900. It controls and manages the entire BS system, provides clock synchronization signals for the BS system and provides the R6 interface for transmission.
- 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.

DOCUMENTS

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

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

- Security Target of Huawei WiMAX BS Software, v0.94, October 10th 2011
- HERT-BBU MML Command Reference V200R007
- Undocumented MML Description WIMAX v0.1, Oct 2011
- Undocumented MML Description HERT-BBU v0.1, Oct 2011
- Installation Guide of Huawei WiMAX BS Software v0.18, Oct 2011
- DBS3900 WiMAX Documentation DRAFT A 20110715
- WiMAX MML Commands Reference V300R0003C01B011
- DBS3900 WiMAX Security Management Guide
- DBS3900 WiMAX Documentation DRAFT B 20111216
- Functional Specification of Huawei WiMAX BS Software v0.47, Oct 2011
- Functional Specification of Huawei BS Annexes v0.1, Oct 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, and
- 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

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

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

- **Huawei WiMAX BS Software, version V300R003C01SPC100**

But for the operation of the TOE it is necessary the disposition of the following components of the TOE environment:

- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- Huawei WiMAX BS Software Operating System: Vxworks, version 5.5.4.
- An M2000 server providing access to the management functions of the TOE via SSL. M2000 version must be V2R11.
- M2000 Mediation Software. The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

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

- The physical structure of a WiMAX BS includes BBU3900 and RRU. BBU3900 is based on HERT hardware platform. HERT BBU is a common platform for wireless multiple products, different boards can be configured according to each product. Beside the hardware support platform subsystem, in most cases only need to configure the BWA Main Processes and Transmission board (BMPT) and BWA Main Processes and Transmission unit (BMPT).
- ASN-GW Access Service Network gateway, providing the routing / switching & control function for WIMAX BS Software via a secure channel enforcing IPSec. There may be a firewall performing NAT between the TOE and the ASN-GW. Different logical ports will then be used, without affecting the overall security of the TOE.
- MS. Mobile station, by air interface data encryption, can share the wireless access through WiMAX network.
- RRU. The RRU is the remote radio unit (RRU) for Huawei Worldwide Interoperability for Microwave Access (WiMAX) base stations (BSs).

EVALUATION RESULTS

The product Huawei WiMAX BS Software, version V300R003C01SPC100, has been evaluated against the "Security Target of Huawei WiMAX BS Software, v0.94", October 10th 2011.

All the assurance components required by the evaluation 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 defined by 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 SSL/TLS to ensure the communications security.
- It is very important the adequate fulfilling of the installation procedures; the installation of TOE may be vulnerable if those procedures are not followed.

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

- 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 abovementioned 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 or moving the TOE to an unsecured state. This problem is although covered with the assumption A.TrustworthyUsers.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei WiMAX BS Software, version V300R003C01SPC100, 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.
- 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.

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

GLOSSARY

AES	Advanced Encryption Standard
ASN-GW	Access Service Network – Gateway
BBU	Base Band Unit
BIN	Huawei's private binary message protocol
BS	Base Station
CC	Common Criteria
CCM	Call Control Management
CCN	Centro Criptológico Nacional
CCRA	Common Criteria Recognition Arrangement
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
FE	Physical acces
FTP	File Transfer Protocol
GE	Physical acces
HERT	Huawei Enhanced Radio Technology
IMS	IP Multimedia Subsystem
LMT	Local Maintenance Terminal
MML	Man-Machine Language
MS	Mobile Station
NAT	Network Address Translation
NE	Network Element
NGN	Next Generation Network
OS	Operating System
PKI	Public Key Infrastructure
RRU	Remote Radio Unit
SFR	Security Function Requirement
SOGIS	Senior Officials Group for Information Systems Security
SSL/TLS	Secure Sockets Layer/Transport Layer Security
TOE	Target Of Evaluation
TSFI	TSF Interface
WIMAX	World Interoperability for Microwave Access

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
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, 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: “Security Target of Huawei WiMAX BS Software, v0.94”, October 10th 2011.

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