REF: 2010-20-INF-810 v1	Created by: CERT8
Target: Público	Revised by: CALIDAD
Date: 21.02.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2010-20 HERT BBU

Applicant: 440301192W HUAWEI

References:

[EXT-1111] Certification request for Huawei HERT BBU Sw Platform

[EXT-1490] Evaluation Technical Report of HERT BBU

The product documentation referenced in the above documents.

Certification report of the product Huawei HERT BBU Software Platform version HERTBBU V200R007C01SPC040B811, as requested in [EXT-1111] dated 21-12-2010, and evaluated by the laboratory Epoche & Espri, as detailed in the Evaluation Technical Report [EXT-1490] received on 16-12-2011.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

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 product Huawei HERT BBU Software Platform version HERTBBU V200R007C01SPC040B811 developed by Huawei Technologies Co., Ltd.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN). Centro Nacional de Inteligencia (CNI).

ITSEF: EPOCHE & ESPRI S.L.

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

Evaluation Level: EAL3 + ALC_CMC.4 + ALC_CMS.4

Evaluation end date: 16/12/2011.

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 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 Huawei HERT BBU Software Platform HERTBBU V200R007C01SPC040B811 product, a positive resolution is proposed.

TOE SUMMARY

Huawei’s Enhanced Radio Technology Base Band Unit (HERT BBU), the TOE is software for the management of base station (BS) devices, such as WIMAX/ W-NodeB/ E-NodeB, and may be other products in the future. It is commonly used as a component throughout a number of Huawei wireless products to offer management functionality for these products.

The TOE is Huawei’s base station software platform (HERT BBU) – in particular the software that provides the Operation Administration and Maintenance (OM) feature and transport management feature for base station devices to their users.

The OM feature possesses the following functions:

- Configuration management;

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Performance management;
- Inventory management;
- Log management;
- Fault management;
- Software management;

The transport management feature possesses the following functions:
- ATM transport management;
- IP transport management;
- Flow separation;

HERT BBU is used in four Huawei's particular products (WIMAX, E-NodeB, TD-NodeB ,W-NodeB and maybe other products in the future). The application-specific functionality of these products is out of scope for this evaluation.

The major security features implemented by HERT BBU and subject to evaluation are:

- Authentication. Operators using local and remote access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

- Access control. HERT BBU 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 HERT BBU.

- Communications security. HERT BBU offers SSL/TLS channels for FTP (File Transfer Protocol), MML (man-machine language which is kind of Command Line Interface), and BIN (Huawei's private binary message protocol) access to the TOE, as well as the IPSec transport channels.

- 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 Access Control List implemented Packet filtering features to restrict resource access via IP address, ports, etc. The features protect the HERT BBU platform shield against various unauthorized access from unauthorized network elements (NEs).

- Security function management. The TOE offers management functionality for its security functionality.

ENAC CERTIFICACIÓN
Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

– 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 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 several requirements as stated by its Security Target, and according to CC Part 2 [CC-P2]. They are requirements for security functions such as access control and identification and authentication.

These functional requirements satisfied by the product are:

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

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

	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 HERT BBU Software Platform, version HERTBBU V200R007C01SPC040B811

Security Target: Huawei HERT BBU Software Platform Security Target Version 1.10 November 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 following Organisational Security Policies are declared in the security target:

P.Audit

The TOE shall provide the following audit functionality:

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

ENAC CERTIFICACIÓN
Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
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, and briefly described below. These same 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.

THREATS

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.

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

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

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 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

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

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.

ARCHITECTURE

PHYSICAL ARCHITECTURE

The TOE is deployed on the boards of Huawei's BBU. The Following figure shows the physical Environment of the Huawei's BBU:

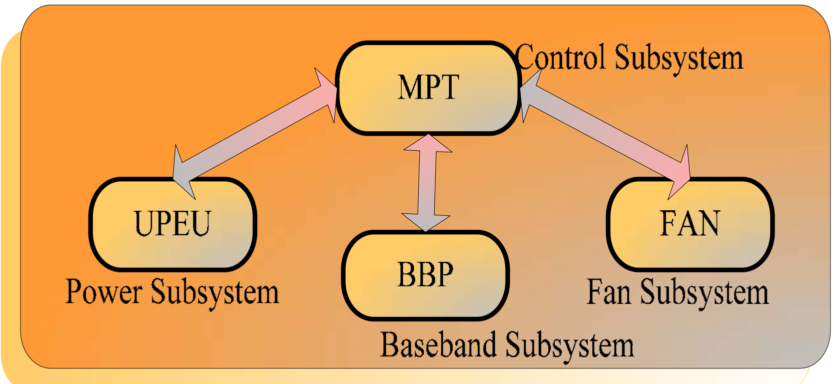

Figure 1 *TOE Physical architecture*

The physical architecture includes the following systems:

Control Subsystem

- The functions of the control subsystem are implemented by the Main Processing and Transmission unit (MPT).
- The control subsystem performs centralized management of the entire BS in terms of OM and signaling processing and provides the system clock.
- All security functions of TOE are deployed on the MPT.

Baseband Subsystem

- The functions of the baseband subsystem are implemented by the Baseband Process Unit (BBP).
- The baseband subsystem processes UL and DL baseband signals.
- The TOE is also deployed on the BBP, but the TOE doesn't provide the security functions on the BBP.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Power Subsystem

- The power module converts +24 V DC or -48 V DC power into the power required by the boards and provides external monitoring ports.
- The TOE is not deployed on this Subsystem.

FAN Subsystem

- The power module controls the fan speed, monitors the temperature of the FAN unit, and dissipates the heat in the BBU.

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:

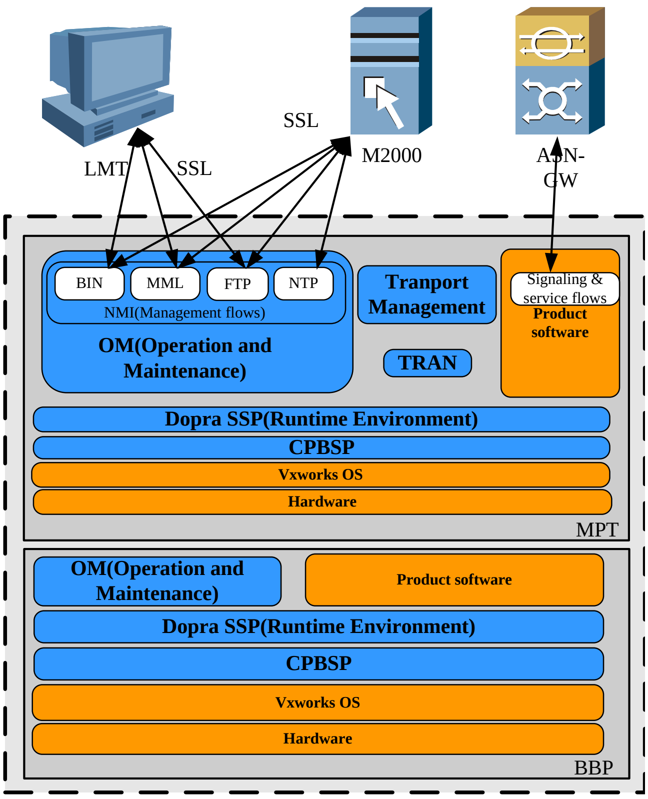

Figure 2 *The TOE logical scope*

The logical scope of the TOE includes local layer which is deployed in BBP and MPT. System control layer which is deployed in MPT.

System control and security management are performed on MPT board via a secure channel enforcing SSL. The management of the functionality of the TOE can be done through different interfaces:

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ENAC CERTIFICACIÓN Nº 45/C-PR110

- BIN/MML through an M2000 server providing management functions to the TOE (in the TOE environment).

- LMT used by users to connect to the TOE for access through HERT BBU via a secure channel enforcing SSL.

DOCUMENTS

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

- Huawei HERT-BBU Software Platform Security Target Version 1.10 November 2011

- CC Installation Guide of HERT BBU (AGD_PRE) v0.90, November 2011

- HERT BBU reference V200R007 June 2011

- HERT BBU BIN&MML Command Group Command Rights V1.2, November 2011

- HERT BBU MML Command Reference V1.3, December 2011

- HERT BBU Undocument MML Description V1.1, November 2011

- Function Description of HERT BBU (ADV_FSP)_V1.20, November 2011

- Functional Specification of Huawei BS Annexes v0.4 November 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.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 is defined by its name and version number:

- Huawei HERT BBU Software Platform Version HERTBBU V200R007C01SPC040B811

The following components were used during the evaluation:

- Hert BBU: HERT BBU V200R007C01SPC040B811
- Switches: No special configuration was needed. The switch must support VLAN configuration.
- M2000 Server: iManagerM2000 Version 2 Release 11 C01 CP1301
- M2000 Client: iManagerM2000V200R011C01SPC130
- LMT: HERTBBU V200R007C01SPC040B811

EVALUATION RESULTS

The product Huawei HERT BBU Software Platform Version HERTBBU V200R007C01SPC040B811 has been evaluated in front of "Huawei HERT BBU Software Platform Security Target. Version 1.10. 2011-11-01".

All the assurance components required by the 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 methodology (augmented with 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 TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

a. The management network shall be a secure network, free of attackers.
b. The fulfilment of the OE.SecurePKI must be strictly observed due to the intensive use of TLS/SSL to ensure the communications security.
c. It is very important the adequate fulfilling of the installation procedures; the installation procedure may be vulnerable if those procedures are not followed.
d. The operators of the product shall use secured computers to interact with the TOE.
e. 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, moving the TOE to an unsecured state (e.g. SET FTPSCLT, SET SSLAUTHMODE, DLD SOFTWARE…). 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 Huawei HERT BBU Software Platform Version HERTBBU V200R007C01SPC040B811, a positive resolution is proposed.

This certification is recognized under the terms of the Recognition Agreement [CCRA] for components up to EAL4 according to the mutual recognition levels of it and the accreditation status of the Spanish Scheme.

The assurance derived from this CR also is covered by the [SOGIS] agreement but only for components until EAL2.

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

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

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.

GLOSSARY

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

ACRONYMS

CCN	Centro Criptológico Nacional
HW	HardWare
SW	SoftWare
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
RMT	Remote Maintenance Terminal
NE	Network Element
CLI	Command Line Interface
GUI	Graphical User Interface
MPU	Main Process Unit

ENAC CERTIFICACIÓN
Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

LPU	Line Process Unit
SFU	Switching Fabric Unit
BTS	Base Transceiver Station
3G	Third Generation
AAA	Authentication, Authorization and Accounting
LTE	Long Term Evolution
MPT	Main Processing & Transmission Unit
MME	Mobility Management Entity
BBU	(Base Station)'s Base Band Unit
OM	Operation and Maintenance
DL	Down Link
UL	Up Link
CPRI	Common Public Radio Interface
RF	Radio Frequency
BBI	Base-Band Interface
LMT	Local Maintenance Terminal
CLI	Command Line Interface
MML	Man-Machine Language
VLAN	Virtual Local Area Network
SGW	Service Gateway
NMS	Network Management System
eNB	evolved Node B (eNodeB), a UMTS base Station
EPC	Evolved Packet Core
IMS	IP multimedia subsystem
NGN	Next Generation Network
LMPT	LTE Main Processing & TransmissionUnit
LBBI	LTE BaseBand processing
UPEU	Universal Power and Environment Interface Unit

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

Common Criteria

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, July 2009.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

SECURITY TARGET

It is published jointly with this certification report the security target,

- “Huawei HERT BBU Software Platform Security Target”. Version 1.10. November 2011. Huawei Technologies Co., Ltd.

.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es