| | |
|---|---|
| REF: 2010-19-INF-811 v1 | Created by: CERT8 |
| Target: Público | Revised by: CALIDAD |
| Date: 21.02.2012 | Approved by: TECNICO |

# CERTIFICATION REPORT

| | |
|---|---|
| File: | 2010-19 GBTS |
| Aplicant: | 440301192W HUAWEI |

References:

[EXT-1110] Certification request of GBTS Software

[EXT-1511] Evaluation Technical Report of GBTS Software.

The product documentation referenced in the above documents.

Certification report of HUAWEI GBTS Software version V100R013C01, as requested by Huawei Technologies in [EXT-1110] dated 21-12-2010, and evaluated by the laboratory EPOCHE&ESPRI, as detailed in the Evaluation Technical Report [EXT-1511] received on December 22nd 2011, and in compliance with [CCRA] and for components up to EAL3 + ALC_CMC.4 + ALC_CMS.4. This CR also is covered by the [SOGIS] agreement 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 GBTS Software version V100R013C01 developed by Huawei Technologies Co., Ltd.

**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**: EAL3+ (ALC_CMC.4, ALC_CMS.4).

**Evaluation end date**: 22/12/2011.

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 GBTS Software version V100R013C01 product, a positive resolution is proposed.

## TOE SUMMARY

The Huawei’s GBTS can be widely used to support the wireless access of home and enterprise users. The Huawei’s GBTS networking supports various access modes, including the FE, GE, optical fibber, microwave access, and satellite.

The GBTS product is a composition of the BSC6900 product and the software running in a BTS3000 unit named equally to the TOE under evaluation GBTS. The BSC6900 is an important Network Element (NE) of Huawei Single RAN solution. It adopts the industry-leading multiple Radio Access Technologies (RATs), IP transmission mode, and modular design. In addition, it is integrated with the functions of the Radio Network Controller (RNC) and Base Station Controller (BSC), thus efficiently maintaining the trend of multi-RAT convergence in the mobile network. The BSC6900 operates as an integrated NE to access the GSM network and includes the functions of the GSM BSC (3GPP R8).

The BSC6900 element is compatible with GSM and UMTS technologies. Nonetheless, one unique configuration and operation mode of the TOE is used and



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

belongs to the obtained from the installation process of the BSC6900 element in GSM mode and the GBTS element.

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

- Authentication: Operators accessing the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords. Also, the TOE connects with the M2000 entity (external management element of the whole communication solution). The communication with the M2000 is protected connection using the SSL/TLS. Also an additional private arithmetic process common to both parties is applied before the elements authentication. Once the M2000 is properly connected the interaction with the TOE is made by the utilization of a special user (EMSCOMM) registered in the BSC6900 element.

- Role_based access control: GBTS and BSC6900 implements role-based access control, limiting access to different management functionality to different roles.

- Auditing: Audit records are created for security-relevant events related to the use of GBTS and BSC6900.

- Communications security: BSC6900 provides SSL/TLS channels (for FTP, HTTP, MML, BIN) to access the TOE.

- Management of security functionality: The TOE offers management functionality for its security functionality.

Digital signature: For the installation and upgrade of GBTS element, the TOE is able to check the software integrity of the package in the BSC6900 unit previous to the installation of the element in order to verify its integrity.

## 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 |



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 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<br>FIA_ATD.1/Local users User attribute definition<br>FIA_ATD.1/Domain users User attribute definition<br>FIA_ATD.1/EMSCOMM user Users attribute definition<br>FIA_SOS.1 Verification of secrets<br>FIA_UID.1 Timing of identification<br>FIA_UAU.1 Timing of authentication<br>FIA_UAU.5 Multiple authentication mechanisms |
| Security Management (FMT) | FMT_MSA.1 Management of security attributes<br>FMT_MSA.3 Static attribute initialization<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| User Data Protection (FDP) | FDP_ACC.1/Local users Subset access control<br>FDP_ACF.1/Local users Security attribute based access control<br>FDP_ACC.1/Domain users Subset access control<br>FDP_ACF.1/ Domain users Security attribute based access control<br>FDP_ACC.1/EMSCOMM user Subset access control<br>FDP_ACF.1/EMSCOMM user Security attribute based access control |
| Trusted path/channels (FTP) | FTP_TRP.1 Trusted path<br>FTP_ITC.1 Inter-TSF trusted channel |
| TOE Access (FTA) | FTA_TSE.1 TOE session establishment |
| Cryptographic Support (FCS) | FCS_COP.1 Cryptographic operation |
| Security Audit (FAU) | FAU_GEN.1 Audit data generation<br>FAU_GEN.2 User identity association<br>FAU_SAR.1 Audit review<br>FAU_SAR.3 Selectable audit review |



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.1 Protected audit trail storage<br>FAU_STG.3 Action in case of possible audit data loss |

# IDENTIFICATION

**Product**: HUAWEI GBTS Software, version V100R013C01

**Security Target:** Huawei GBTS Software Security Target, version 1.30, December 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 TSF shall be able to generate an audit record of the auditable events, which associate with the identity of the user that caused the event. The TSF shall protect the stored audit records in the audit trail from unauthorized deletion. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

**P.RoleManagement**
Different people access the TSF needs to be divided according to different roles with different permissions, as far as possible the user has the minimum required permissions.

# 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.


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

**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 core 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.OperatingSystem**
It is assumed that the Operating System of the TOE' environment is secure.

**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. |
| 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.


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

**Threats by Eavesdropper**

| Threat: T1. InTransitConfiguration | |
|---|---|
| Attack | An eavesdropper in the management network succeeds in accessing the content of the BSC6900 data 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 BSC6900 software/patches while transferring, violating its confidentiality or integrity. |
| Asset | A1.Software and patches |
| Agent | Eavesdropper |

**Threats by Internal Attacker**

| Threat: T3.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: T4.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.



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

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

**OE.Physical**
The TOE (i.e., the complete system including attached peripherals, such as a console) shall be protected against unauthorized physical access.

**OE.NetworkSegregation**
The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network.

**OE.OperatingSystem**
The Operating System of the TOE' environment is secure.

**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.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.SecurePKI**

There exists 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

The TOE is composed of the BSC6900 unit and the GBTS unit. The main elements of the BSC6900 are:

- **OMU:** The OM enables the management and maintenance of the BSC6900 in the following scenarios: routine maintenance, emergency maintenance, upgrade, and capacity expansion.

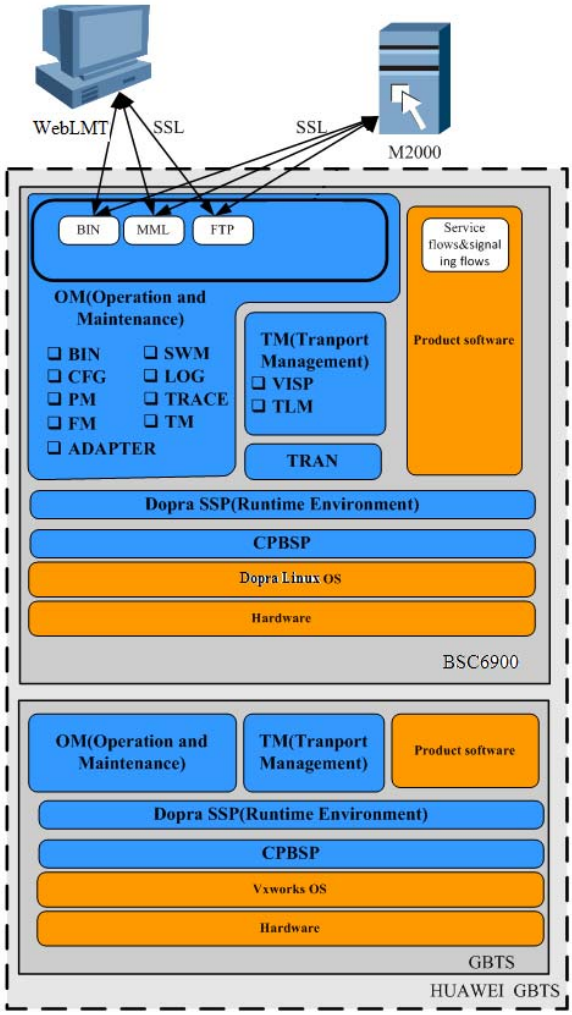
- **Interface Processing:** The interface processing provides transmission ports and resources, processes transport network messages, and enables interaction between the BSC6900 internal data and external data.



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

The GBTS is considered as one element (running in the GTMU part of the BTS3000 system) which main functionalities provide: transport configuration, traffic forwarding, DHCP and VLAN separation.

The logical boundary is represented by the elements in blue color. But in the GBTS and BSC6900, there are also the other functions.




TOE Software architecture

For the BSC6900 element it is depicted in the picture the following features:

a. The interface processing (depicted in the picture as Transport Management) is in charge of controlling the flow (datagrams) between the BSC6900, GBTS and the Core Network. This control is performed by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine. Also, a session establishment control is performed in order to accept or deny connections. In case of failure, the fault tolerance procedure will switch the active interface board with the stand-by interface board.



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

b. The OMU is in charge of the system control and security managements of the BSC6900. This management is performed via a secure channel enforcing SSL/TLS. Also, it controls the flow of the connection with the M2000 and WebLMT elements. The same fault tolerance procedure is implemented in the OMU, so in case of failure, the switch with the stand-by board will remains the system operative.

For the GBTS element it is depicted in the picture:

a. The OMU is in charge of the system control. All the GBTS operations are performed in this board, so no important functionality is executed in the rest of boards of the BTS3000 system.
b. The interface processing (depicted in the picture as Transport Management) is in charge of the flow (datagrams) between the BSC6900 and GBTS.

## DOCUMENTS

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

- Huawei GBTS Software Security Target, version 1.30, December 2011
- Guide to Deploying the Security Feature of BSC6900V900R013-0001, v 1.01, August 2011
- CC Installation Guide of BTS3000V100R013C01 GBTS (AGD_PRE), v 1.01, November 2011
- CC Installation Guide of BSC6900 (AGD_PRE), version 1.01, November 2011
- (For Customer)BSC6900 GU Product Documentation (V900R013C01SPC010_Draft A)(HDX)-EN, Draft A 0.2,
- CC Certification: BSC6900 Functional Specification (ADV_FSP), version 1.11, November 2011
- Undocument MML Description (EN)(BSC6900), 1.0, November 2011
- CC Certification: BSC6900 BIN & MML Commands Operational Rights, v 1.0, November 2011
- Functional Specification of Huawei BS ANNEXES, v0.1, November 2011

## TOE 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.



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 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 is 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.



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

### *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: code Injection, SQL injection, brute force, session establishment control bypass, session unlocking bypass, monitoring, misuse, covert channels, denial of service, memory disclosure, audit.

## EVALUATED CONFIGURATION

The TOE is defined by its name and version number:

- **HUAWEI GBTS Software version V100R013C01**

## EVALUATION RESULTS

The product HUAWEI GBTS Software version V100R013C01 has been evaluated against the "Huawei GBTS Software Security Target, version 1.30", December 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 no exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

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.



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

d. 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.
e. The guidance 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.

The normal operation of the TOE implies that the human users (local and domain users) can only access the TOE through the WebLMT interface. It is the EMSCOMM user, representing the M2000, the one which accesses all the other ports (MML, BIN, Notification Performance …) defined for the TOE. In this sense, it should be controlled by the secure PKI that only the M2000 entity possesses a certificate to access these other ports. And, the TOE will allow only the access for human user access for the WebLMT.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product HUAWEI GBTS Software version V100R013C01, a positive resolution is proposed.

This certification is recognised under the terms of the Recognition Agreement [CCRA] for components up to EAL3+ (ALC_CMC.4, ALC_CMS.4) 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.

## 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.



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

**Informal** - Expressed in natural language.

**Protection Profil**e - 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 |
| **LAN** | Local Area Network |
| **PP** | Protection Profile |
| **SW** | SoftWare |
| **SSH** | Secure Shell |
| **SSL** | Secure Socket Layer |
| **ST** | Security Target |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |

## 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.

[CEM] Common Evaluation Methodology for Information Technology Security:



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

Introduction and general model, Version 3.1, r3, July 2009

## SECURITY TARGET

It is published jointly with this certification report the security target, **"Huawei GBTS Software Security Target, version 1.30", December 2011**.



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