



REF: 2010-24-INF-831 v1

Created by: CERT3

Target: Público

Revised by: CALIDAD

Date: 07.03.2012

Approved by: TECNICO

CERTIFICATION REPORT

File: 2010-24 Huawei BSC6900 Multimode Base Station Controller (MBSC)
Software V900R013C01SPC010

Applicant: 440301192W HUAWEI

References:

- [EXT1115] Certification request of Huawei BSC6900 MBSC Software V900R013C01SPC010
 - [EXT1487] Evaluation Technical Report of Huawei BSC6900 MBSC Software V900R013C01SPC010
 - The product documentation referenced in the above documents
-

Certification report of the product HUAWEI BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010, as requested by Huawei Technologies in [EXT-1115], dated 21-12-2010, and evaluated by the laboratory EPOCHE&ESPRI, as detailed in the Evaluation Technical Report [EXT-1487] received on December 22nd 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.....	3
TOE SUMMARY	3
SECURITY ASSURANCE REQUIREMENTS.....	4
SECURITY FUNCTIONAL REQUIREMENTS	5
IDENTIFICATION.....	5
SECURITY POLICIES.....	6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT.....	6
CLARIFICATIONS ON NON-COVERED THREATS.....	7
OPERATIONAL ENVIRONMENT FUNCTIONALITY	8
ARCHITECTURE	9
DOCUMENTS	11
PRODUCT TESTING.....	12
PENETRATION TESTING.....	13
EVALUATED CONFIGURATION.....	13
EVALUATION RESULTS.....	13
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM.....	14
CERTIFIER RECOMMENDATIONS	14
GLOSSARY	15
BIBLIOGRAPHY	15
SECURITY TARGET.....	16



EXECUTIVE SUMMARY

This document constitutes the Certification Report for the product HUAWEI BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010, 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: Common Criteria 3.1 R3 - EAL3+ (ALC_CMC.4; ALC_CMS.4).

Evaluation end date: 22/12/2011.

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 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 BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010, a positive resolution is proposed.

TOE SUMMARY

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&UMTS network and integrates the functions of the GSM BSC and the UMTS RNC.

The BSC6900 is compatible with GSM and UMTS technologies. Nonetheless, one unique configuration and operation mode of the TOE is used. This belongs to the obtained from the installation process. So, the configuration of TOE according to the security features provided is always the same, independently of the technology used in operation (GSM or UMTS).

The major security features implemented by the TOE 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.

- Role-based access control: 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 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 of GBTS managed element, the TOE is able to check the software integrity of the package 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-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 [CC-P2].

Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling FIA_ATD.1/Local users User attribute definition FIA_ATD.1/Domain users User attribute definition FIA_ATD.1/EMSCOMM user Users 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 users Subset access control FDP_ACF.1/Local users Security attribute based access control FDP_ACC.1/Domain users Subset access control FDP_ACF.1/ Domain users Security attribute based access control FDP_ACC.1/EMSCOMM user Subset access control FDP_ACF.1/EMSCOMM user Security attribute based access control
Trusted path/channels (FTP)	FTP_TRP.1 Trusted path 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 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 BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010.

Security Target: Huawei BSC6900 Multimode Base Station Controller Software Security Target, version 1.07, December 20th 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 BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010, 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.

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.

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.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product HUAWEI BSC6900 Multimode Base Station Controller Software, version V900R013C01SPC010, although the agents implementing attacks have the attack potential according to the BASIC of CC-EAL3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threat agents can be categorized as either:

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

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

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.

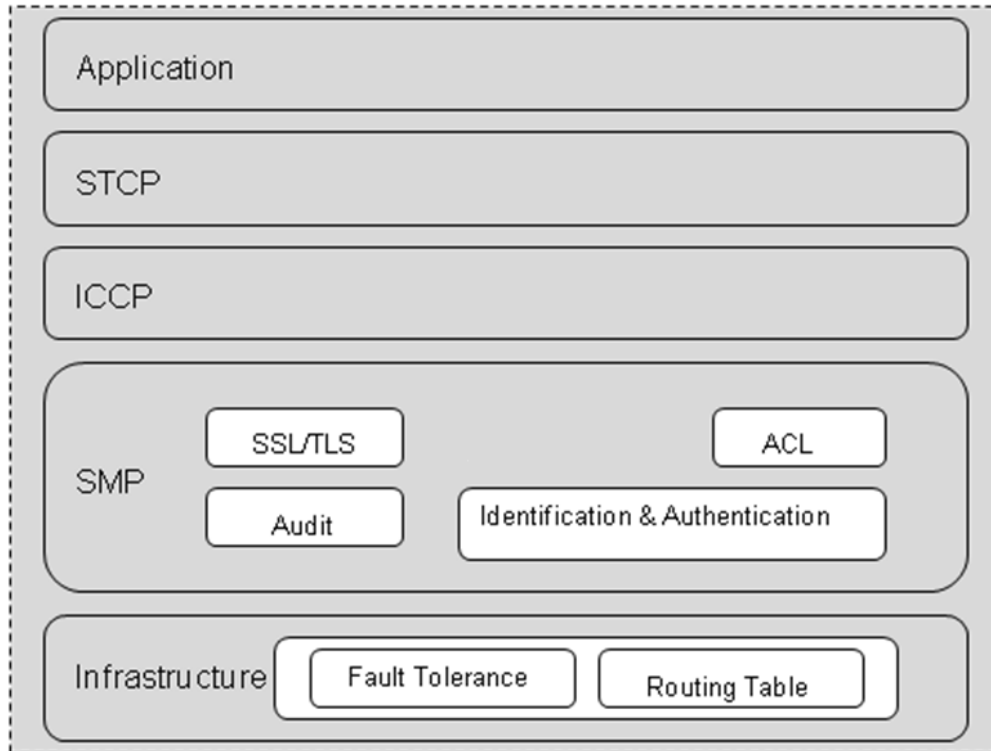
OE.SECUREPKI

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

ARCHITECTURE

The TOE is composed of the following two elements:

- **OMU:** The OMU 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.



TOE Software architecture

The specific functionality detailed in the white boxes is executed in a distribute way. The modules SSL/TLS, ACL, Audit, Identification & Authentication and Fault tolerance are executed in the OMU board. The modules relating with the routing table and connection filtering out of the management network are executed on the interface board.

The following table shows the functions of each layer in the BSC6900 software architecture.

Layer	Functions
Infrastructure	a) Provides the hardware platform and hides the lower-layer hardware implementation. b) Hides the differences for operating systems, and provides enhanced and supplementary functions for the system.
Service Management Plane (SMP)	c) Provides the OM interface to perform the OM functions of the system.



Layer	Functions
Internal Communication Control Plane (ICCP)	<p>d) Transfers internal maintenance messages and service control messages between different processors, thus implementing efficient control over distributed communication.</p> <p>e) Operates independent of the infrastructure layer.</p>
Service Transport Control Plane (STCP)	<p>f) Transports the service data on the user plane and control plane at the network layer between NEs.</p> <p>g) Separates the service transport technology from the radio access technology and makes the service transport transparent to the upper-layer service.</p> <p>h) Provides service bearer channels.</p>
Application	<p>i) Implements the basic functions of network element service control and controls the upper-layer service, such as call processing, mobility management, and RRM.</p> <p>j) Hides the topology characteristics of various resources in the network and in the equipment.</p> <p>k) Provides the resource access interface, hides the distribution of internal resources and network resources, maintains the mapping between the service control and resource instance, and controls the association between various resources.</p> <p>l) Manages the resources and OM status, responds to the resource request from the upper layer, and hides the resource implementation from the upper layer.</p> <p>m) Isolates the upper-layer services from the hardware platform to facilitate the hardware development.</p>

DOCUMENTS

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

- Huawei BSC6900 Multimode Base Station Controller Software Security Target, version 1.07, December 20th 2011.



- Guide to Deploying the Security Feature of BSC6900V900R013-0001, v1.01, August 2011.
- CC Installation Guide of BSC6900 (AGD_PRE), version 1.01, November 2011.
- BSC6900 GU Product Documentation (V900R013C01SPC010_Draft A)(HDX)-EN, Draft A 0.2, December 2011 (for customers).
- 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.
- CC Certification: BSC6900 Functional Specification (ADV_FSP), version 1.11, 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, 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 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: 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, that it is just software, is defined by its name and version number:

- **HUAWEI BSC6900 Multimode Base Station Controller Software version V900R013C01SPC010.**

EVALUATION RESULTS

The product HUAWEI BSC6900 Multimode Base Station Controller Software version V900R013C01SPC010 has been evaluated against the “Huawei BSC6900 Multimode Base Station Controller Software Security Target”, version 1.07, December 20th 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 [CC-P3] and [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 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 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. 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 BSC6900 Multimode Base Station Controller Software version V900R013C01SPC010, a positive resolution is proposed.

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



- The TOE's consuming organizations should develop and implement a Security Policy to review and delete TOE's expired user accounts. The TOE is not able to deny access to users whose accounts have an expired password. This SFR is not declared within the TOE's Security Target.
- The TOE's consuming organizations should develop and implement a Security Policy to notify and force users to reset their user password in case changes are made in the TOE's Password Policy. The TOE is not able to notify users or enforce modifications in the user accounts if a modification in the password policy is made after a user password is created. This SFR is not declared within the TOE's Security Target.

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

CC	Common Criteria
CCN	Centro Criptológico Nacional
CCRA	Common Criteria Recognition Arrangement
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
MBSC	Multimode Base Station Controller
NE	Network Element
RRM	Radio Resource Management
SFR	Security Function Requirement
SOGIS	Senior Officials Group for Information Systems Security
TOE	Target Of Evaluation
TSFI	TOE Security Function Interface

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 BSC6900 Multimode Base Station Controller Software Security Target, version 1.07”, December 20th 2011.