MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF:	2010-15-INF-681 v1	Creado:	CERT2
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	05.07.2011	Aprobado:	JEFEAREA

CERTIFICATION REPORT

Expediente: 2010-15
Datos del solicitante: 440301192W HUAWEI

References:

EXT - 1098	Certification Request of Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00). 30/08/2010. Huawei Technologies Co., Ltd
EXT - 1257	Evaluation Report for Huawei Carrier Grade Platform (CGP) software. (Unique version identifier: CGP V100R005C00) ETRHUAW001_ETR_M0. LGAI-Applus
EXT - 1273	Evaluation Report for Huawei Carrier Grade Platform (CGP) software. (Unique version identifier: CGP V100R005C00) ETRHUAW001_ETR_M1. LGAI-Applus
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.
SOGIS	European Mutual Recognition Agreement of IT Security Evaluation Certificates v3.0, January 2010.

Certification report for the Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604, as requested by Huawei Technologies in [EXT-1098] dated 30-8-2010, and evaluated by the laboratory LGAI-APPLUS, as detailed in the Evaluation Technical Report [EXT-1273] received on May 23rd 2011, and in compliance with [CCRA] and for components up to EAL3. This CR also is covered by the [SOGIS] agreement but only for components until EAL2.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

Table Of Contents

Executive Summary

This document constitutes the Certification Report for the product for the Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604 developed by Huawei Technologies.

Developer/manufacturer: Huawei Technologies.

Sponsor: Huawei Technologies.

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

ITSEF: LGAI Technological Center. APPLUS.

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

Evaluation Level: EAL3.

Evaluation end date: 23/05/2011.

All the assurance components required by the level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604, a positive resolution is proposed.

TOE Summary

The TOE is Huawei's Carrier Grade Platorm, software for the management of cellular core network devices, such as Home Location Registers, Mobile Softswitch Centers, Service GPRS Support Nodes, or Call Session Control Functions. It is commonly used as a component throughout a number of Huawei networking products to offer management functionality for these products

The central (server) side of Carrier Grade Platform (CGP) runs within a physical Operation and Management Unit (OMU) on top of a Linux operating system. Operation and Management Unit (OMU)s are boards (blades) that get inserted into network device cabinets (racks) which also contain application-specific boards, resulting in a product offering. Remote clients (a GUI, called Local Maintenance Terminal (LMT) client, and a web-based interface) are available for management access to the server. This evaluation of CGP covers the use of CGP in six particular products, the Huawei CSC3300, HLR9820, MSOFTX3000, SGSN9810, ATS9900, and HSS9820. The application-specific functionality of these products is out of scope for this evaluation.

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

- Authentication. Operators using the GUI client or a web browser to access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

- Role-based access control. CGP implements role-based access control, limiting access to different management functionality to different roles as defined in administrator-defined access control associations.

- Lawful Interception (LI) support. CGP offers management functionality for Lawful Interception (LI), including access control mechanisms that enforce the separation of LI operators from other operators.

- Communications security. CGP offers Secure Socket Layer (SSL)/Transport Layer Security (TLS) channels for File transport protocol (FTP), Hypertext transfer protocol (HTTP), and Simple object access protocol (SOAP) access to the OMU, as well as the encryption of X1/X2 channels for LIG communication. This includes the possibility to restrict remote sessions to the CGP server to specific client Internet Protocol (IP) addresses.

- Auditing. Audit records are created for security-relevant events related to the use of CGP.

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

The operational environment of the TOE comprises, on the server side, an operating system that runs within the OMU board hardware and hosts both the TOE and a relational database (which is part of the operational environment as well) used by the TOE to store configuration and audit data.

The LMT client part of the TOE runs on top of a Windows operating system.

In a larger context, the remaining parts of the product that integrates the TOE as its management component is also considered part of the operational environment.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil EAL3, 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.3, ALC_CMS.3, 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 information flow control, identification and authentication.

These functional requirements satisfied by the product are:

Security Audit (FAU)	FAU_GEN.1 Audit data generation	FAU_GEN.1
	FAU_GEN.2 User identity association	FAU_GEN.2
	FAU_SAR.1 Audit review	FAU_SAR.1
	FAU_SAR.3 Selectable audit review	FAU_SAR.3
	FAU_STG.3 Action in case of possible audit data loss	FAU_STG.3
Cryptographic Support (FCS)	FCS_COP.1: Cryptographic operation	FCS_COP.1

User Data Protection (FDP)	FDP_ACC.1: Subset access control	FDP_ACC.1
	FDP_ACF.1: Security attribute based access control	FDP_ACF.1
Identification and Authentication (FIA)	FIA_AFL.1: Authentication failure handling	FIA_AFL.1
	FIA_ATD.1: User attribute definition	FIA_ATD.1
	FIA_SOS.1: Verification of secrets	FIA_SOS.1
	FIA_UAU.2: User authentication before any action	FIA_UAU.2
	FIA_UID.2: User identification before any action	FIA_UID.2
Security Management (FMT)	FMT_MSA.1: Management of security attributes	FMT_MSA.1
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3a
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3b
	FMT_SMF.1: Specification of Management Functions	FMT_SMF.1
	FMT_SMR.1: Security roles	FMT_SMR.1
Protection of the TSF (FPT)	FPT_ITT.1: Basic internal TSF data transfer protection	FPT_ITT.1
TOE Access (FTA)	FTA_TSE.1: TOE session establishment	FTA_TSE.1
Trusted Path/Channels (FTP)	FTP_TRP.1: Trusted path	FTP_TRP.1

Identification

Product: Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604.

Security Target: Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Security Target. v0.28 2011/03/09.

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

Evaluation Level: CC v3.1 r3 EAL3

Security Policies

There are no security policies declared in the ST.

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.

In this TOE ST there are only these assumptions to be considered:

- **A.PhysicalProtection** It is assumed that the TOE and its operational environment (in particular, the network device that the TOE is a component of, but also the workstation that is hosting the client part of the TOE) are 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 application (or, public) networks that the network device hosting the TOE serves.
  This includes the assumption that the operational environment implements measures that ensure that the source IP address in remote client session establishment requests has not been tampered with, and that no bogus OMU servers exist in the management network.

- **A.Support** The operational environment must provide the following supporting mechanisms to the TOE:
  - Reliable time stamps for the generation of audit records.
  - The database that stores the data of TOE must be protected and available.

Threats

This section describes the security threats to the TOE:

- **T.AccountabilityLoss** Records of security-relevant actions of users for forensic and accountability purpose are not created properly.

- **T.Eavesdrop** An eavesdropper (remote attacker) in the management network that is served by the TOE is able to intercept, and potentially modify or re-use, information assets that are exchanged between TOE (LMT) and non-TOE (WebUI) clients, and the TOE server part (OMU).

- **T.UnauthenticatedAccess** A user who is not a user of the TOE gains access to the TOE.

- **T.UnauthorizedAccess** A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized to access.

Any other threats not included in this list are not necessarily resisted by the TOE.

Operational environment objectives

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 environment are the following:

- **OE.Administration** Those responsible for the operation of the TOE and its operational environment must ensure that only authorized users have access to the OMU, and in particular to the part of the TOE and its data that is running on the OMU. This includes ensuring that audit records

stored in the operational environment are protected against unauthorized access, and that cryptographic keys and certificates are properly managed to support the communications security mechanisms implemented by the TOE.
This also includes the restriction of physical access to the network device that contains the OMU to authorized personnel, and making the OMU unavailable to access from the consumer/application networks served by the network device.
The TOE must be operated in its evaluated configuration as specified in this ST and the guidance that is part of the TOE.

- **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.
  - The database that stores the data of TOE must be protected and available.

- **OE.Users** 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.

TOE Architecture

The TOE is Huawei’s Carrier Grade Platform software (Unique version identifier: CGP V100R005C00) – in particular the software that provides the Operation Administration and Maintenance (OAM) functionality for core network devices to their users. The TOE is implemented based on a client/server architecture – the server functionality is located in the network device itself, while a client GUI – commonly referred to as Local Maintenance Terminal (LMT) – can be run on PCs for remote management of the device.

Physically, the server part of the TOE is located on an OMU board, a type of Universal Process Blade that is located within the network device. The TOE server communicates product-internally with application-specific boards (Network Elements) of the product in order to provide management and maintenance functionality for the device.

Remote communication between LMT client and the OMU of a device is based on TCP/IP. In addition to using the proprietary link between the LMT client software and the OMU, the OMU also serves a web interface – commonly referred to as WebUI – that remote users can access directly using their web browsers in order to obtain performance statistics, access the OMU via a console provided by a virtual KVM switch, perform software upgrades, and download a copy of the LMT GUI.

Also, a SOAP interface is available for communication with the operational environment (namely Huawei’s Enterprise Management System, a separate product offering), as well as an SNMPv3 interface.

Via these interfaces, the OMU offers management functionality for the network device. To be more precise, the LMT GUI implements security function management. The management functionality offered by the WebUI is not security-relevant in terms of the TOE – but authentication and communications security provided for the interface are.

The TOE supports Lawful Interception (LI) technology. CGP offers the management of LI functionality via X1/X2 channels. In particular, this includes the configuration of communication parameters that instruct CGP how to interoperate with a Lawful Interception Gateway (LIG) in the operational environment for exchanging control messages and alerts.

The TOE stores configuration data, such as user attributes and access control associations, as well as audit records, in a configuration database in the operational environment.

Documents

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

- Huawei Technologies Co., Ltd. CGP Customer Product Information, User Guides, v1, 2009-08-12

- Huawei Technologies Co., Ltd. CGPV100R005C00 CGP Function Description, v1.4, 2011-02-10

- Huawei Technologies Co., Ltd. ETSI Lawful Interception, User Guides, v N/A, N/A

- Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Security Target, Security Target, v0.28

TOE Testing

The manufacturer has developed testing for the TOE TSF. All these tests have been performed by the manufacturer in their location and facilities with success.

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.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target.

It is been checked also that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator examined the evaluation evidences and determined that the developer has been provided in the test documentation a cross-table that unambiguously maps each test with a TSFI of the functional specification.

The TOE’s configuration that has been tested meets what has been described in the ST by the developer. All the products that the TOE can manage have been configured (once at a time) and different tests (developer and evaluator) have been executed while the TOE is configured for the specific product.

While the developer test plan is focused on cover the entire TSF and on demonstrating his correct implementations, the evaluator test approach is to gain in depth respect the developer tests.

All the developer’s tests were executed changing the managed product to observe if there were differences on the behaviour of the TOE produced by the managed product. All the results obtained during this stage were as expected and, actually, the TOE behaviour is the same independently of the product under management.

The evaluator executed the tests and updated the test documentation with new devised tests. The evaluator verified that the obtained results were agreed with expected results.

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 independent penetration testing devised several test cases covering attacks including SQL Injection, Xpath injection, cross-site Scripting, cross-site request forgery, buffer overflows, race conditions, replay attacks, MiTM attacks, brute force or IP spoofing.

During the penetration testing the evaluator used the product configured as indicated in the guidance. The CGP is used in six commercial products configurations, so the evaluator executed the test cases over all the configurations and in all the products.

The testing effort validates the public interfaces available to potential attacker.

The evaluator did not find either exploitable vulnerabilities or residual vulnerabilities in the operational environment as a result of independent penetration testing.

Evaluated Configuration

The TOE is defined by its name and version number:

- **Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604.**

Evaluation Results

The product Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604 has been evaluated in front of the "Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Security Target, Security Target, v0.28", 2011/03/09.

All the assurance components required by the level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Comments & Recommendations from the Evaluation Team

There are no recommendations.

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the Huawei Carrier Grade Platform (CGP) software (Unique version identifier: CGP V100R005C00) with the following patch V100R005C00SPC604 product, a positive resolution is proposed.

This certification is recognised under the terms of the Recognition Agreement [CCRA] for components up to EAL3 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.

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

CC	Common Criteria
CM	Configuration Management
CGP	Carrier Grade Platform
FTP	File transport protocol
GUI	Graphical User Interface
HTTP	Hypertext transfer protocol
IP	Internet Protocol
LI	Lawful Interception
LMT	Local Maintenance Terminal
MML	Man Machine Interface
NTP	Network Time Protocol
OMU	Operation and Management Unit
OSP	Organizational Security Policies
SFR	Security Functional Requirement
SOAP	Simple object access protocol
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSFI	TOE Security Functionality Interface
TSF	TOE Security Functionality

CGP	Carrier Grade Platform

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

Security Target

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

"Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Security Target, Security Target, v0.28", 2011/03/09