REF: 2012-4-INF-1418 v1 | Created by: CERT10
Target: Expediente | Revised by: CALIDAD
Date: 14.01.2015 | Approved by: TECNICO

CERTIFICATION REPORT

File: 2012-4 HUAWEI CGP v1.r5.c1

Applicant: 440301192203821 HUAWEI Technologies Co., Ltd.

References:

[EXT-1683] Certification request of HUAWEI CGP v1.r5.c1

[EXT-1416] Evaluation Technical Report of HUAWEI CGP v1.r5.c1.

The product documentation referenced in the above documents.

Certification report of the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506, as requested in [EXT-1683] dated 13-02-2012, and evaluated by the laboratory Applus LGAI Technological Center S.A., as detailed in the Evaluation Technical Report [EXT-1416] received on 19-12-2014.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506.

The TOE is Huawei's Carrier Grade Platform, a 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 CGP runs within a physical Operation and Management Unit (OMU) on top of a Linux operating system. OMUs 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 LMT client) are available for management access to the server.

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

- Authentication. Operators using the GUI client 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.
- Communications security. CGP offers SSL/TLS channels for FTP, and 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 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.

The remaining parts of the assembly products, where the TOE is located, are part of the operational environment.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

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

ITSEF:Applus LGAI Technological Center S.A..

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

Evaluation Level: EAL3.

Evaluation end date: 10/12/2014.

All the assurance components required by the evaluation level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory LGAI Technological Center S.A. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3, as defined by the EAL3 and the Common Criteria v3.1 R3 (CC_P1, CC_P2, CC_P3) and the CEM v3.1 R3.

Considering the obtained evidences during the instruction of the certification request of the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506, a positive resolution is proposed.

TOE SUMMARY

The TOE is Huawei’s Carrier Grade Platform – 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, it using the proprietary link between the LMT client software and the OMU.

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 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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

Authentication

The TOE authenticates its users via individual user names and passwords. The TOE is able to enforce password policies as well as “lockout” policies to deter password guessing attacks.

Further, it is possible to limit login of specific users to specific time frames and to define expiry dates for accounts and passwords.

The TOE entertains two user domains: LI user domain and service user domain.

LI user domain includes two roles: LI user super user, and administrator-defined roles of LI user.

Service user domain includes two roles: service user super user, and administrator-defined roles of service user.

LI users differentiate between service users, i.e. the operators responsible for the day-to-day operation of the TOE, and LI users who can access the TOE in order to configure lawful interception functionality to be executed by network elements.

By means of implementing a separate user ID space described above, the TOE ensures that the realms of service and LI management are kept completely separate – service users do not know about the existence of and cannot interfere with the operations of LI users, and vice versa.

Access control

The TOE offers the management of network devices.

The TOE implements access control that allows limitation of access both in terms of operations that a user is authorized to perform and in terms of objects that a user can perform these operations on.

The TOE allows the definition of User Groups, as well as Command Groups and Managed Object Groups, in order to define roles that can be assigned to users.

The TOE differentiates between service users and LI users by implementing a separate access control functionality for two user domains.

Communications security

The TOE offers SSL/TLS encryption for communication between the LMT client and the OMU, and for communication between the operational environment and the TOE via SOAP.

The TOE is furthermore able to restrict session establishment to administrator-specified IP source addresses in LMT client requests.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

CGP implements encryption for the FTPS protocol that allows users to access the FTP server hosted by CGP.

The TOE also implements encryption of the communication between its Lawful Interception module and a Lawful Interception Gateway in the operational environment, commonly referred to as the X1 / X2 interfaces.

Auditing

The TOE records and reviews audit data, which is stored in the database and it can be queried using TOE-provided tools (i.e., via the LMT client).

The TOE differentiates between service users and LI users, service users can use the LMT client to review the audit records available in the database for everything except LI-related actions. LI users can review only audit records related to LI functionality and actions initiated by LI users.

Security function management

The following means are provided by the TOE for management of security functionality:

- User and group management
- Access control management (by means of defining command groups, managed object groups, and association of users with particular managed elements, managed objects, and commands)
- Supporting of SSL for communications security.
- Enabling and disabling of the LI feature.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3, according to the Common Criteria v3.1 R3 (CC_P1, CC_P2, CC_P3).

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R3 (CC_P1, CC_P2, CC_P3):

SECURITY FUNCTIONAL CLASS	FAMILY/COMPONENT	FUNCTIONAL REQUIREMENT
SECURITY AUDIT (FAU)	**FAU_GEN.1**	FAU_GEN.1 AUDIT DATA GENERATION
	FAU_GEN.2	FAU_GEN.2 USER IDENTITY ASSOCIATION
	FAU_SAR.1	FAU_SAR.1 AUDIT REVIEW
	FAU_SAR.3	FAU_SAR.3 SELECTABLE AUDIT REVIEW
	FAU_STG.3	FAU_STG.3 ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS
CRYPTOGRAPHIC SUPPORT (FCS)	**FCS_COP.1A**	FCS_COP.1: CRYPTOGRAPHIC OPERATION
	FCS_COP.1B	FCS_COP.1: CRYPTOGRAPHIC OPERATION
USER DATA PROTECTION (FDP)	**FDP_ACC.1**	FDP_ACC.1: SUBSET ACCESS CONTROL
	FDP_ACF.1	FDP_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL
IDENTIFICATION AND AUTHENTICATION (FIA)	**FIA_AFL.1**	FIA_AFL.1: AUTHENTICATION FAILURE HANDLING
	FIA_ATD.1	FIA_ATD.1: USER ATTRIBUTE DEFINITION
	FIA_SOS.1	FIA_SOS.1: VERIFICATION OF SECRETS
	FIA_UAU.2	FIA_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION
	FIA_UID.2	FIA_UID.2: USER IDENTIFICATION BEFORE ANY ACTION

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

SECURITY MANAGEMENT (FMT)	**FMT_MSA.1**	FMT_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES
	FMT_MSA.3A	FMT_MSA.3: STATIC ATTRIBUTE INITIALIZATION
	FMT_MSA.3B	FMT_MSA.3: STATIC ATTRIBUTE INITIALIZATION
	FMT_SMF.1	FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS
	FMT_SMR.1	FMT_SMR.1: SECURITY ROLES
PROTECTION OF THE TSF (FPT)	**FPT_ITT.1**	FPT_ITT.1: BASIC INTERNAL TSF DATA TRANSFER PROTECTION
TOE ACCESS (FTA)	**FTA_TSE.1**	FTA_TSE.1: TOE SESSION ESTABLISHMENT
TRUSTED PATH/CHANNELS (FTP)	**FTP_TRP.1**	FTP_TRP.1: TRUSTED PATH

IDENTIFICATION

Product: Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506.

Security Target: Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 Security Target Version 2.0.

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

Evaluation Level: Common Criteria v3.1 R3 (CC_P1, CC_P2, CC_P3) EAL3.

SECURITY POLICIES

This Security Target defines no Organizational Security Policies.

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.

Physical

Assumption 01: 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.

Personnel

Assumption 02: 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 belong to administrators group are assumed to be fully trustworthy and capable of operating the TOE in a secure manner abiding by the guidance provided to them. Note that the users who do not belong to administrators group or unauthorized, are untrustworthy and not eligible for this assumption.)

Connectivity

Assumption 03: 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.

Assumption 04: 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.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506, although the agents implementing attacks have the

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

attack potential according to the "Basic" of 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 threats covered by the security properties of the TOE are categorized below.

Threat 01: T.AccountabilityLoss

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

Threat 02: 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) client and the TOE server part (OMU).

Threat 03: T.UnauthenticatedAccess

A user who is not a user of the TOE gains access to the TOE.

Threat 04: 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.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Environment objective 01: 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Environment objective 02: 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.

Environment objective 03: 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. Note that the users who do not belong to administrators group or unauthorized, are untrustworthy and not eligible for this environmental objective.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is Huawei's Carrier Grade Platform – in particular the software that provides the Operation Administration and Maintenance (OAM) functionality for core network devices to their users. As depicted in Figure 1, 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

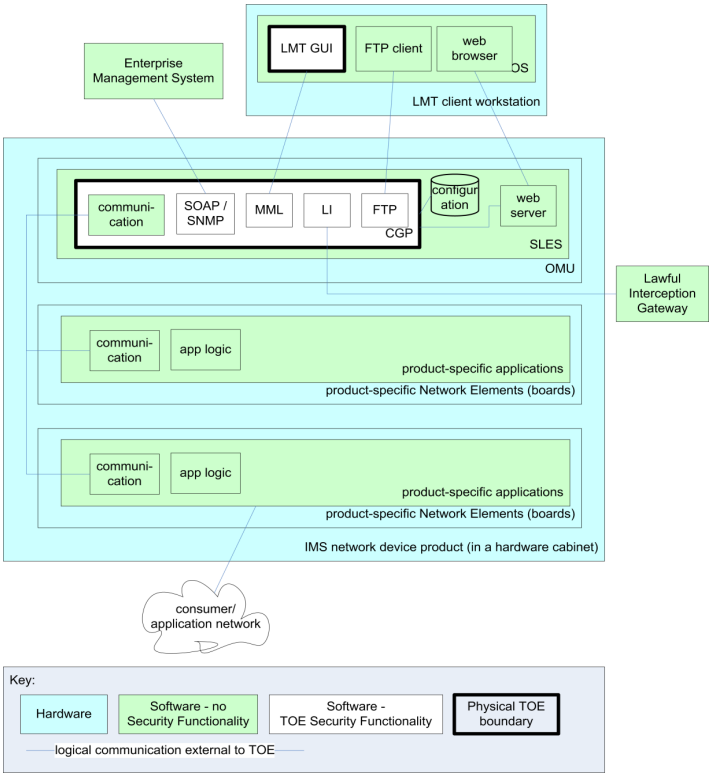

Figure 1: TOE architecture and boundaries

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, it using the proprietary link between the LMT client software and the OMU.

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 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

PHYSICAL ARCHITECTURE

The TOE is software only. It is used in a number of Huawei's core network devices that are comprised of elements compatible with the Advanced Telecommunications Computing Architecture (ATCA). Within these networking devices, the OMU board hosting the server part of the TOE is a common board that is paired with different combinations of application-specific boards (network elements). The server part of the TOE is the actual Carrier Grade Platform software running on the OMU that implements the generic device management capabilities for these products.

For the guidance of TOE, the registered personnel can download the guidance from Huawei's website: http://support.huawei.com.

The guidance of the TOE comprises the following documents:

- CGP Product Documentation, V100R005C01, Huawei Technologies Co., Ltd., 2013-02-21, v02.
- LI User Guidance, V100R005C01, Huawei Technologies Co., Ltd., 2013-02-21, v02.

Non-TOE hardware/software/firmware required by the TOE

The server part of the TOE depends on the following hard- and software in its operational environment:

- the cabinet (rack and subrack) housing the OMU and application-specific boards, comprising an actual network device product assembly
- the physical OMU board providing processing resources and physical interfaces
- the operating system running on the OMU, SuSE Linux Enterprise Server 10
- a database product used to store configuration and other maintenance data, PROTON Database based on postgreSQL

The client part of the TOE is comprised of the LMT client, running on a designated LMT workstation. The web browser needed to access the web-based WebUI provided by the server is part of the operational environment.

The client part of the TOE depends on the following hard- and software in its operational environment:

- the workstation providing the processing resources and physical interfaces for the LMT client, or a web browser for access to the WebUI
- Windows 2000/XP/Vista as operating system

The TOE is distributed as a component of a larger product assembly, and the guidance that is part of the TOE is integrated into the product manuals of the individual product.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

The product assemblies supported by this evaluation of CGP are:

- Huawei ENS, offering the Domain Name System (DNS) and Telephone Number Mapping (ENUM) in IMS networks
- Huawei CCF, a Charging Gateway for IMS networks, offering an interface for offline charging
- Huawei UGC3200, offering Media Gateway Control Function (MGCF) in IMS networks and Gateway Mobile Switching Center (GMSC) in mobile networks
- Huawei SPG2800, a universal service provisioning gateway, offering the universal northbound service provisioning interface for the IMS components
- Huawei MRP6600, a multimedia resource function processor, is used to carry multimedia resources and supports multimedia services
- Huawei SAE-HSS9820, offering Home subscriber server (HSS) in the evolved packet core (EPC) network and Home location register (HLR) in mobile networks
- Huawei UPCC, a Unified Policy and Charging Controller(UPCC) for IMS networks

The LMT client is shipped with the respective network device.

Please note that the application-specific functionality offered by these product assemblies is not subject to this evaluation. The TOE is only concerned with the provision of operational and maintenance functionality that is common to these products.

DOCUMENTS

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

The guidance of the TOE comprises the following documents:

- CGP Product Documentation, V100R005C01, Huawei Technologies Co., Ltd., 2013-02-21, v02.
- LI User Guidance, V100R005C01, Huawei Technologies Co., Ltd., 2013-02-21, v02.

PRODUCT TESTING

The evaluator has tested all the SFRs defined through the TOE TSFIs. It has been checked that the obtained results conform to the expected results. The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation Manuals.

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result. During the evaluation process it has been verified each unit test checking that the security

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506 it is necessary the disposition of the following software components:

The evaluated configuration of CGP is based on the physical and logical scope and security functions described above. In addition, the following configuration specifics are applicable to the TOE:

- CGP supports standby configurations between two OMUs for the same product. This functionality has not been evaluated.
- CGP supports LI user security management, during the evaluation SET TTSEC command must be executed to enable the LI user security function.
- CGP supports DES encryption for various communication channels, such as the channel between CGP and a Lawful Interception Gateway, for legacy reasons. This evaluation does not cover the use of the DES algorithm for LI feature.
- CGP supports DES for encryption of configuration data. During the evaluation CGP must be configured so that AES is used instead of DES for LI feature.
- CGP supports COMMON communication between LMT clients and the OMU. This evaluation does not cover the use of the COMMON communication. During the evaluation CGP must be configured so that SSL communication mode is used instead of COMMON communication mode.
- CGP supports DES communication between the operational environment (EMS server) and the OMU in SNMP interface. During the evaluation CGP must be configured so that the parameters SNMP Protocol version as SNMPv3, and Private protocol as DES (CBC-DES).
- CGP supports security policy, during the evaluation security policy data must be configured and parameters value should be:
    - Password policy = Enable
    - Change password upon first login = Enable

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

  - Password expiration warning period(day), customized account default as 5 and build-in account default as 20
  - Minimum password length = 8
  - Character set, enable all character sets.
  - Enforce password history = 5
  - Enforce password days = 10
  - Minimum password age, customized account default as 5 and build-in account is not available.
  - Account lockout policy = Enable
  - Number of login attempts before lockout = 5
  - Count reset interval(minute) = 10
  - Lockout duration(minute) = 30
  - Unused account lockout period(day), customized account default as 30 and build-in account is not available.
  - Repeated login rejection policy = Enable
- CGP supports session establishment management. During the evaluation the parameters value of Account validity period, Password validity period, Start login time, and End login time must be specified when adding the new user through the ADD USER command.
- CGP supports workstation management. During the evaluation workstation access control function must be enabled through the SET WS command.
- CGP supports network time protocol, during the evaluation the parameter values of Authentication flag must be configured as Yes, and other parameters value should match with the NTP server side when adding the NTP server data through the ADD NTPSVR command.

Regarding the hardware components, the only requirement is that they shall support the software elements previously detailed.

EVALUATION RESULTS

The product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506 has been evaluated against the Security Target Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 Security Target Version 2.0.

All the assurance components required by the evaluation level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory LGAI Technological Center S.A. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3, as defined by the Common Criteria v3.1 R3 and the CEM v3.1 R3.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The evaluator evaluated the TOE Huawei Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 and its evidences from 07/08/2012 to 26/11/2014.

Each assurance class has a positive evaluation result Pass.

During the evaluation process, the developer has provided evidences and resolutions as soon as required.

The Observation Reports were related to the documentation evidences, no vulnerabilities have been found in any part of the TOE. Therefore, no issue was detected according to the standard and evidences used for the evaluation. The product fulfilled the whole set of Security Functional Requirements established in the Security Target.

There is no additional recommendation from the Laboratory in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

Since all the classes of the evaluation have a Pass verdict, the overall evaluation verdict is Pass. Therefore, from the Laboratory point of view, the product is considered to be compliant with the CC standard with an assurance level of EAL 3.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506, a positive resolution is proposed.

During the evaluation, the publication of the Heartbleed vulnerability leads the Laboratory to examine its impact on the TOE. The version of openSSL running on the TOE was not affected by the vulnerability. Nevertheless, the Laboratory made a search of public vulnerabilities in order to discard any potential security flaw.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

OC	Organismo de Certificación
TOE	Target Of Evaluation

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 Carrier Grade Platform (CGP) Version 1 Release 5 Customization 1 Security Target Version 2.0.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es