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

REF:	2010-22-INF-764 V1	Created:	CERT2
Distribution:	Expediente	Reviewed:	TECNICO
Date:	21.11.2011	Approbed:	JEFEAREA

CERTIFICATION REPORT FOR FOR HUAWEI INTEGRATED MANAGEMENT APPLICATION PLATFORM VERSION 3 RELEASE 1 C05 SPC500

Dossier: 2010-22 IMAP V3 R1

References:

EXT-1113 Certification Request of iMAP Version 3 Release 1 C05 SPC500. 13/12/11. HUAWEI.

EXT-1389 Evaluation Report for iMAP Version 3 Release 1 C05 SPC 500. HUA-IMAP-ETR v2.0. 08/09/2011. EPOCHE&ESPRI

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 of Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500, as requested by HUAWEI in [EXT-1113] dated 13-12-2011, and evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report [EXT-1389] received on September 22nd 2011, and in compliance with [CCRA] for components up to EAL4 and [SOGIS] for components up to EAL2.

Table Of Contents

SUMMARY 3
TOE SUMMARY 4
SECURITY ASSURANCE REQUIREMENTS 5
SECURITY FUNCTIONAL REQUIREMENTS 6
IDENTIFICATION 7
SECURITY POLICIES 7
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 7
THREATS 8
OPERATIONAL ENVIRONMENT OBJECTIVES 9
TOE ARCHITECTURE 10
SOFTWARE ARCHITECTURE 10
DOCUMENTS 11
TOE TESTING 11
PENETRATION TESTING 12
EVALUATED CONFIGURATION 13
EVALUATION RESULTS 13
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 13
CERTIFIER RECOMMENDATIONS 14
GLOSSARY 14
BIBLIOGRAPHY 16
SECURITY TARGET 16

Summary

This document constitutes the Certification Report for the software application *Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500* developed by HUAWEI.

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.

Protection Profile: No conformance to any protection profile is claimed.

Evaluation Level: EAL3 + (ALC_CMC.4, ALC_CMS.4).

Evaluation end date: 22/09/2011.

All the assurance components required by the level EAL3+ (augmented with ALC_CMC.4, ALC_CMS.4) have been assigned a “PASS” verdict. Consequently, the laboratory (EPOCHE & ESPRI) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3+(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 Integrated Management Application Platform Version 3 Release 1 C05 SPC500, a positive resolution is proposed.

TOE Summary

This TOE is a software platform that provides the basic functionality of an OSS (Operation Support System). This application might be used by operators to manage network elements (NEs - hardware devices) in telecommunication domain.

The TOE is a Client-Server kind of application by itself, providing the basic functionality of an OSS. This TOE implements basic functions of OSS security features, including account based system access control that enforces only authenticated user can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking; Alarm processing is used to collect and analyze NEs alarms; system management to manage services of the OSS its own.

To build a complete OSS system, the developers will need to implement new service modules like performance management/configuration management that are more specific to individual product domain.

As described in its Security Target, the TOE provides the security level of EAL3+ augmented with ALC_CMC.4 and ALC_CMS.4.

The TOE needs the following hardware and software requirements being satisfied:

- A Sun M4000 hardware system with Sun Solaris 10 operating system and Sybase 15 database system installed to be deployed on.
- A PC with Windows XP operating system installed is required to run the software client.
- The physical network connection between the client and server is mandatory.

All these additional hardware and software components required for operating environment are not included in this evaluation.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil EAL3, augmented with the components ALC_CMC.4 (Production support, acceptance procedures and automation) and ALC_CMS.4 (Problem tracking CM coverage), according to CC Part 3 [CC-P3].

Assurance Class	Assurance Components
Security Target	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 ASE_TSS.1 TOE summary specification
Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary ADV_TDS.2 Architectural design
Guidance	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Life Cycle	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model
Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Vulnerability Analysis	AVA_VAN.2 Vulnerability analysis

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 security audit, user data protection, user identification and authentication, or security management.

The security functional requirements satisfied by the product are:

- FAU: Security Audit
  - FAU_GEN.1
  - FAU_GEN.2
  - FAU_SAR.1
  - FAU_SAR.2
  - FAU_SAR.3
  - FAU_STG.3

- FIA: Identification and Authentication
  - FIA_AFL.1
  - FIA_ATD.1
  - FIA_SOS.1
  - FIA_UID.2
  - FIA_UAU.2

- FMT: Security Management
  - FMT_MSA.1
  - FMT_MSA.3
  - FMT_MSA.4
  - FMT_SMR.1
  - FMT_SMF.1

- FDP: User data protection
  - FDP_ACC.2
  - FDP_ACF.1

- FCS: Cryptographic Support
  - FCS_COP.1

- FTA: TOE Access
  - FTA_TAB.1
  - FTA_TSE.1

- FPT: Protection of the TSF
  - FPT_ITT.1

Identification

Product:	Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500
Security Target:	Huawei Integrated Management Application Platform Security Target. Version 0.63. 2011-08-24.
Protection Profile:	None
Evaluation Level:	CC v3.1 r3 EAL3+ (ALC_CMC.4, ALC_CMS.4).

Security Policies

There is not any additional security policy defined in the Security Target that organizations shall implement to achieve the assurance level claimed on it.

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.

The following assumptions are considered in this TOE ST:

A.PhysicalProtection It is assumed that the hardware system (usually a unix server) which the components of the TOE reside in is protected against unauthorized physical access.

A.NetworkSegregation It is assumed that the sub-network which the TOE reside in is separate from the application (or, public) networks. The communications with the TOE are performed through a firewall. See section 1.4.2.2 Logical scope of the ST for more information.

A.OperatingSystem It is assumed that the operating system for the TOE has been hardened properly and patched in time, so there is no security weakness, and thus protected against unauthorized access.

A.DataBase It is assumed that the database system used by TOE has been hardened properly and patched in time, so there is no security weakness, and thus protected against unauthorized access.

A.Administrator It is assumed that the superuser admin and the users that belong to the SMManagers and Administrator groups behave correctly and do not perform harmful operation in the TOE. Also, the users of the underlying operating system.

Threats

This section describes the security threats to the TOE:

Threat	Attack
T.UnauthenticatedAccess	**Attacker:** Unauthenticated user **Asset:** A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack:** A user without a valid user account of the TOE successfully bypass the authentication process and pretend to be an authenticated user of the TOE, then gain access to the assets. Depend on the authorization of the user he pretend to be, he may compromise the availability, integrity and confidentiality of all the assets.
T.UnauthorizedAccess	**Attacker**: Authenticated User **Asset**: A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack**: An authenticated user successfully bypass the authorization control of the TOE and gain access to the assets he is not authorized to. he may compromise the availability, integrity and confidentiality of all the assets.

T.Eavesdrop	**Attacker**: Network attacker **Asset**: A.NE Connectivity Data/ A. Configuration Data / A.Alarm Data **Attack**: A network attacker from management network successfully intercept the data communication of the TOE and compromise the confidentiality of NE Connectivity, alarm and configuration Data and the integrity of NE Connectivity and alarm Data.
T. BehaviorDeny	**Attacker**: Authenticated User **Asset**: A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack**: An authenticated user perform an authorized operation by means or by mistake, compromise the availability and integrity of the assets(for example, delete NE connectivity data), and deny what he has done.

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.Physical

The hardware system which the TOE server is running on 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. A firewall shall be installed in the environment.

OE.OperatingSystem

The operating system which the TOE server is running on shall be protected against unauthorized access.

OE.DataBase	The database system used by the TOE shall be protected against unauthorized access.
OE.Administrator	The superuser admin and the users that belong to the SMManagers and Administrator groups of the TOE should behave correctly and should not perform harmful operation in the TOE. Also, the users of the underlying operating system.

TOE Architecture

This section will introduce the TOE from a physical architectural view and a software architectural view.

Software Architecture

The software architecture of the TOE is an enhancement of the traditional Client/Server (C/S) architecture, which consists of three layers:

- AS, Application Server
- DS, Desktop Server
- Client

Note that the Application Server is the main functional layer, the OSS features of data collecting, data processing and data configuration are implemented in this layer, and system authentication and authorization features are also included as well.

The Desktop Server layer can be considered as a data cache layer, it provides data query feature. Client layer only communicates with desktop server layer, the data retrieving requests are fulfilled in DS while the data modification requests are passed down to AS layer.

The Client layer is the graphic user interface (GUI) of OSS system, it provides data presentation, and data query and data configuration interfaces to end users.

Physical Architecture

The TOE need the following hardware and software requirements being satisfied: A Sun M4000 hardware system with Sun Solaris 10 operating system and Sybase 15 database system installed to be deployed on. A PC with Windows XP operating system installed is required to run the software client. Meanwhile, the physical network connection between the client and server is mandatory.

The environment for TOE comprises the following components:

- Computer hardware with OS system to run the TOE's AS and DS software

- Personal Computer used by administrators and operators to run the TOE's client software to access the system function
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- Firewall: all the accesses to the TOE are performed through a firewall. Only the following communications are allowed by the firewall:
  a. TCP interface(with SSL enabled): this interface is used in communication between GUI client and the server of the TOE (XRPC protocol).
  b. SFTP interface: the TOE use this interface to communicate between the GUI and the Server.
  c. SNMPv3 interface: the TOE use this interface to communicate with upper management system and act as SNMPv3 client.
  d. CAU interface for updating the software.
  e. Hedex interface for providing on-line help.

All these hardware and software components required for operating environment are not included in this evaluation.

Documents

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

- iMap Help, Library version 01 May 2011
- Huawei Integrated Management Application Platform Installation Guide V300R001C05SPC500 August 2011
- iMAP_Help Version 3 Release 1 C05 SPC500 August 2011

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.

The testing approach was oriented to test the interfaces (external and between subsystems) as they are detailed in the functional and design descriptions of the

TOE. The setup and procedures for the test cases allows demonstrating that the behaviour of each subsystem was checked.

It is been checked also 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 declared functionality was tested. The evaluator verified that TSFI were tested in the developer's test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The evaluator repeated a subset of the test cases specified by the developer in the test documentation and ITSEF compared the obtained results with those obtained by the developer and documented in each associated report. The results obtained when repeating the tests were the same than the results obtained by the developer.

The evaluator also carried out independent testing activities. The main objective of the testing performed by the evaluator was to check the requirements stated in the Security Target using the TSFIs and also taking into account the subsystems definition.

Moreover, the evaluator has carried out tests with parameters of the TOE (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 functionality management stated in FMT_SMF.1 requirement was also tested in all the tests deployed by the evaluator.

The results of independent tests were successful 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 the analysis of all the interfaces of the TOE.

The evaluator performed an analysis, trying to bypass, tamper or misuse of the security mechanisms and functionalities implemented in the TOE. The vulnerability analysis paid special attention to the TOE communications, testing and checking their security.

The TOE configuration used in the penetration testing was consistent with the configuration described in the security target.

The evaluator did not find any exploitable vulnerability in the operational environment as a result of independent penetration testing for this assurance level (EAL3+ALC_CMC.4+ALC_CMS.4).

Evaluated Configuration

The TOE is defined by its name and version number:

- **Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500**

Evaluation Results

The product Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500 has been evaluated in front of the "Huawei Integrated Management Application Platform Security Target. Version 0.63.", 2011-08-24.

All the assurance components required by the level EAL3+ (augmented with ALC_CMC.4, ALC_CMS.4) have been assigned a "PASS" verdict. Consequently, the laboratory (EPOCHE & ESPRI) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology (augmented with ALC_CMC.4, ALC_CMS.4), as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Comments & Recommendations from the Evaluation Team

This section describes 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.

The following usage recommendations are given by the evaluator:

- The operational environment shall be installed properly, overall the firewall to access the TOE has to be configured adequately.

- The SUN server and the database, where the TOE lies, shall be well-configured and patched.

- The admin and the users, who belong to the SMManager group and the Administrator group, shall behave correctly. Moreover, they shall trust the other trusted users, given that it is possible to impersonate users being one of the trusted users.

- It is important to know that is possible to perform more operations sending XRPC commands than through the GUI. i.e. The GUI shows less information to the user than the allowed one.

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the Huawei Integrated Management Application Platform Version 3 Release 1 C05 SPC500, a positive resolution is proposed.

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

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

Additionally the Certifier recommends potential users to consider the following:

- It must be stated that due to design prescriptions, the client side subsystem is able to write logs to the audit record if user decides so. The method to write these distributed system log entries might be unreliable, so these entries must not be fully trusted. These entries are marked in the audit record with prefix *“Added by DS”* to easily differentiate them from the trusted ones.

- Recommendations provided in the TOE’s help documentation must be considered in order to properly understand how the TOE implements certain security functionalities.

- User must pay attention to the comments and recommendations provided by the evaluation team.

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.

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 Integrated Management Application Platform Security Target. Version 0.63. 2011-08-24.”