REF: 2010-21-INF-765 V1
Distribution: Expediente
Date: 21.11.2011

Created: CERT2
Reviewed: TECNICO
Approbed: JEFEAREA

CERTIFICATION REPORT FOR iMANAGER M2000 VERSION 2 RELEASE 11 C01 CP1301

Dossier: 2010-21 Huawei M2000

References:

EXT-1112 Certification Request of iManager M2000 version 2 Release 11 C01 CP 1301. 13/12/10. HUAWEI.

EXT-1390 Evaluation Report for iManager M2000 version 2 Release 11 C01 CP 1301. HUA-M2000-ETR Version 2.0. 16-09-2011 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 the software application iManager M2000 version 2 Release 11 C01 CP 1301, as requested by Huawei Technologies Co. Ltd., in [EXT-1112] dated 13-12-2010, and evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report [EXT-1390] received on September 22nd 2011, and in compliance with [CCRA] for components up to EAL4 and [SOGIS] for components up to EAL2.

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Table Of Contents

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

Summary

This document constitutes the Certification Report for the software application iManager M2000 version 2 Release 11 C01 CP 1301 developed by Huawei Technologies Co., Ltd.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN). 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 iManager M2000 version 2 Release 11 C01 CP 1301, a positive resolution is proposed.

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

TOE Summary

The software application iManager M2000 version 2 Release 11 C01 CP 1301 (M2000 V200 R011 C01 CP1301) provides centralized operation and maintenance (OM) for Huawei's mobile network element management solution, provides external interfaces for interoperability with other systems. The core of iManager M2000 version 2 Release 11 C01 CP 1301 is the iMAP Platform, the software for managing the mobile network elements.

Note: The TOE version is the result of applying the patch V200R011C01CP1301 to the product version V200R011C01SPC130 (that is also called main version).

Note: It is also used the acronym M2000 as TOE reference in this Certification Report, in the Security Target and ancillary documents for CC evaluation.

The iMAP platform within M2000 software application provides extensive security features, including account based system access control that enforced only authenticated users can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking.

M2000 provides additional security features. These include centralized users management for network elements (NE); auditing of security-relevant activities and users' operations; as well as encrypted transmission between network elements and iManager M2000, between client and server of iManager M2000.

The major security features implemented by iManager M2000 and subject to evaluation are:

- User Role management
- Access Control
- Auditing
- IP-based ACL
- Encrypted transmission
- User session management
- Security function management

The M2000 server software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces.

The M2000 can manage new NEs after the corresponding mediation software is installed. The M2000 adopts an open structure so that it can manage the devices of core network (CN), system architecture evolution (SAE), IP multimedia subsystem (IMS), and radio networks of various technologies such as global system for mobile (GSM), wideband code division multiple access (WCDMA), code division multiple

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

access(CDMA), worldwide interoperability for microwave access(WiMAX) and long term evolution (LTE).

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.

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

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

- FDP: User data protection
  - FDP_ACC.2/iMAP
  - FDP_ACC.2/MML
  - FDP_ACF.1/iMAP
  - FDP_ACF.1/MML

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

- FMT: Security Management
  - FMT_MSA.1/iMAP
  - FMT_MSA.1/MML
  - FMT_MSA.3/iMAP
  - FMT_MSA.3/MML
  - FMT_SMF.1
  - FMT_SMR.1

- FPT: Protection of the TSF
  - FPT_ITT.1

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

- FCS: Cryptographic Support
  - FCS_COP.1/SNMP
  - FCS_COP.1/NE
  - FCS_CKM.1

- FTP:Trusted Path/Channels
  - FTP_TRP.1

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Identification

Product: iManager M2000 version 2 Release 11 C01 CP 1301
Security Target: iManager M2000 Security Target. Version 1.20. 08-09-2011.
Protection Profile: None
Evaluation Level: CC v3.1 r3 EAL3+ (ALC_CMC.4, ALC_CMS.4).

Note: The TOE version is the result of applying the patch V200R011C01CP1301 to the product version V200R011C01SPC130 (that is also called main version).

Security Policies

There is one additional security policy defined in the Security Target that organizations shall implement to achieve the assurance level claimed on it. This organizational security policy is:

- **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 provide the audit records in a manner suitable for the user to interpret the information.

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:

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

A.Physical	The TOE is operated in a physically secure and well managed environment. It is assumed that the software platform of the TOE including such as Solaris OS, Sybase are protected against unauthorized physical access. It is assumed that the database Sybase is protected against data file damage. It is assumed that secured connections to Solaris OS are always enabled to access to Sun server.
A.NetworkElement	It is assumed that the managed network elements can support the SSL connection with the TOE, and the private interface defined by Huawei.
A.NetworkSegregation	It is assumed that the network interface in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks. The communications with the TOE are performed through a firewall. See section 1.4.2 Environment in the Security Target for more information
A.Connection	It is assumed that the connection between the external system (also NEs) and the TOE is secured in a trusted network which is protected against attacks.
A.AdministratorBehaviour	It is assumed that the super user admin and the users that belong to the SMManagers and Administrator groups will behave correctly and will not perform any harmful operation in the TOE. Also, the users of the underlying operating system.

Threats

This section describes the security threats to the TOE:

T.UnauthenticatedAccess

Threat: T.UnauthenticatedAccess	
Attack	An attacker who is not a user of the TOE, gains access to the TOE, modifies and compromises the confidentiality of the TSF

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

	data and the OM data.
Asset	TSF data, OM data
Agent	Attacker

T.UnauthorizedAccess

Threat: T.UnauthorizedAccess	
Attack	An unauthorized user may gain unauthorized accesses to the TOE and compromises the confidentiality and the integrity of the TSF data and OM data. Also perform non-authorized operations in the NEs.
Asset	TSF data, OM data
Agent	Unauthorized user

T. Eavesdrop

Threat: T.Eavesdrop	
Attack	An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and NEs, between the client and server of the TOE and between the server and the SNMP client.
Asset	OM data; TSF data
Agent	Eavesdropper

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.NetworkElements The operational environment shall ensure that the managed network elements can support the SSL connection with the TOE, and the private interface

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

	defined by Huawei.
OE.Physical	The TOE (i.e., the complete system including attached peripherals, such as Sun workstation, disk array) 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.NetworkCommunication	The operational environment should provide secured network for the communication between the TOE and external systems.
OE.Database	The operational environment shall protection to the database for storage of security data against unauthorized physical access.
OE.AdministratorBehaviour	The super user admin and the users that belong to the SMManagers and Administrator groups will behave correctly and will not perform any harmful operation in the TOE. Also, the users of the underlying operating system.

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

TOE Architecture

The iManager M2000 software consists of the main version software and mediation software. The main version software implements system functions, and the mediation software is used for the adaptation of different NE interfaces. The M2000 can manage new NEs after the corresponding mediation software is installed.

The protocols with NEs are listed as followed:

- MML/BIN basing on Socket channel
- SOAP + MML

The M2000 provides standard common object request broker architecture (CORBA), simple network management protocol (SNMP), file, and alarm streaming interfaces. In addition, the M2000 allows for interoperability with other systems.

Software Architecture

The iManager M2000 is developed basing on the iMAP software platform.

The TOE consists of three parts to support centralized network management.

- NE mediation software
- Server software
- Client software

Note that the NE mediation software is to communicate with network elements and adapt the different interface for different network elements. The interface with network elements includes such as SSL connection, file transfer protocol(FTP), FTPS. The adapted network elements can include the elements of the CN, IMS, GSM, WCDMA, SAE, CDMA, WiMAX and LTE networks, which are developed by Huawei.

During the evaluation, the NEs mediation software tested have been SAE-HSS and BSC6900 UMTS.

The server software is to provide the services for client software, and external interfaces for the external system.

The client software is responsible for providing Graphic User Interface (GUI) to access to M2000 server.

Physical Architecture

This section describes the Supported Platforms and hardware Environment of the iManager M2000.The physical environment includes the following parts:

- The Server

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

- The Client

The server provides physical platform for server software and NE mediation software of the TOE. The physical structure of M2000 server is composed of a third-party disk array and a workstation with either Unix or Linux operating system (OS) and database software.

The client provides physical platform for client software of the TOE. The physical structure is composed of Private Computer with Windows OS software.

The table below shows the typical configuration of the hardware and software for the TOE physical environment.

Device Type	**Device Description**	**Quantity**	**Configuration Description**
Server	Server Module(SUN M4000, 4 CPU, Single Server)	1	Number of CPUs: 2 CPU clock frequency: 2.53 GHz Memory: 16 GB Local disk: 2 x 146 GB Disk array: one S2600 (each S2600 consists of twelve 450 GB hard disks) Operating system: Solaris 10 Database: Sybase 15.0.2
PC	Client	1	CPU: E5300 or above Memory: 2 GB Hard disk: 160 GB Accessories: DVDRW-Integrated Ethernet adapter-Integrated audio adapter-Built-in sound box-19" LCD Operating system: Windows XP professional (or a later version)

The NEs which can be managed by the TOE and supports different communication protocols with the TOE, are part of the environment of the TOE.

During the evaluation, the NEs tested have been SAE-HSS and BSC6900 UMTS.

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

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

Environment

The environment for TOE comprises the following components:

- The underlying platform for the evaluation is limited to single-server system on Sun Platform;The databases and tools(including such as sftp/ftp/ftps server) should be contained in the underlying platform.
- Network element developed by Huawei, providing secure sockets layer (SSL) connect and supporting file transfer protocol over SSL (FTPS).
- The third party system or tools providing connection to the TOE through external interface including the protocols such as SNMP, CORBA, FTP, MML.
- Remote PCs used by administrators to install the client part of the TOE and connect to the TOE for access through GUI interfaces.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on Sun workstation within the TOE via a secure channel enforcing secure shell (SSH).
- Physical networks, such as Ethernet subnets, interconnecting various networking elements.
- Firewall: all the accesses to the TOE are performed through a firewall. Only the following communications are allowed by the firewall:
    - TCP interface(with SSL enabled): this interface is used in communication between GUI client and the server of the TOE (Corba and XRPC protocol).
    - AT&NIC Website.
    - OMMonitor communication.
    - SFTP interface: the TOE use this interface to communicate between the GUI and the Server.
    - SNMPv3 interface: the TOE use this interface to communicate with upper management system and act as SNMPv3 client.
    - CAU interface for updating the software.
    - Hedex interface for providing on-line help.
    - Communications with the NEs.

Configuration

Based on TOE scope described so far, a list of configuration is to be added:

- SSL connection and secure file transfer protocol (SFTP) for file transfer via the GUI interface between M2000 server and client should be activated.
- Encrypted transmission between network elements and M2000 should be activated.
- For secure transmission to M2000 server via GUI, the SSL should be used to connect the M2000 server.

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

Documents

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

- M2000 Product Documentation (Solaris10) V200R011C01 Version Draft B September 2011
- iManager M2000 V200R011C01SPC130 Upgrade Guide (Command Line Mode) issue 01 July 2011
- iManager M2000 V200R011C01CP1301 Upgrade Guide (Command Line Mode) issue 01 August 2011
- M2000 Operation Guide for Mediation (Only for Single System) issue 02 June 2010
- M2000-CME Product Documentation V200R011C01 Version Draft C July 2011
- iManager M2000-CME V200R011C01CP1001 Upgrade Guide issue 01 August 2011
- iManager M2000-CME V200R011C01SPC100 Component Installation Guide issue 01 July 2011
- M2000 Operation Guide for Setting Chroot for File Transfer and Log Setting issue 1.01 August 2011
- Solaris System Security Hardening Operation Guide v 2.0 February 2011

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

TOE Testing

The tests performed by both the evaluator and the developer were based in the TSFIs description included in the functional specification and the design documents for depth testing.

The TOE configuration used to execute the functional tests (TSFIs) and depth testing was consistent with the evaluated configuration according to security target [ST120].

The installation procedure followed is explained in the documentation provided by the developer with the TOE with the detail required and it was followed to place the TOE in a secure state for testing.

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

The process verified each unit test, checking that the security functionality that covers was identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests were 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 also was checked that the obtained results during the tests fitted or corresponded to the previously estimated results.

The **evaluator** repeated a subset of the test cases specified by the developer in the test documentation and compared the obtained results with those obtained by the developer and documented in each associated report.

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 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.

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

To choose the tests, the evaluator chose as criteria, test all the security related classes, test the classes with a right associated and test the methods that are security concerned.

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 and subsystems interactions.

The evaluator performed an analysis such as that all the declared interfaces and SFRs of the TOE have been tested trying to circumvent the security functionality of the TOE.

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

Finally, 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).

TOE Configuration

The TOE is defined by its name and version number:

- **iManager M2000 version 2 Release 11 C01 CP 1301**

Note: The TOE version is the result of applying the patch V200R011C01CP1301 to the product version V200R011C01SPC130 (that is also called main version).

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

Evaluation Results

The product iManager M2000 version 2 Release 11 C01 CP 1301 has been evaluated in front of the “iManager M2000 Security Target. Version 1.20. 08-09-2011”.

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 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 Evaluation Team states that the TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- 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 network where the NEs are installed shall be trustful.
- 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/CORBA commands than through the GUI. i.e. The GUI shows less information to the user than the allowed one.

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

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the iManager M2000 version 2 Release 11 C01 CP 1301, a positive resolution is proposed.

This certification is recognized 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:

- 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 may 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

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,

- **“iManager M2000 Security Target. Version 1.20. 08-09-2011”. Huawei Technologies Co., Ltd.**

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es