MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2014-43-INF-1560 v1	Created by: CERT9
Target: Expediente	Revised by: CALIDAD
Date: 16.03.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2014-43 ASSET MANAGER WITH CONNECT-IT

Applicant: HP Hewlett-Packard development Company

References:

[EXT 2621] Certification request of ASSET MANAGER WITH CONNECT-IT

[EXT 2898] HP Asset Manager v9.50 with Connect-It v9.60 Evaluation Technical Report, v 1.0, 30-12-2015.

The product documentation referenced in the above documents.

Certification report of the product “HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)”, as requested in [EXT 2621] dated 04-11-2014, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT 2898] received on 30/12/2015.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)”.

The TOE is a software-only TOE and provides an organized way to manage the life cycle of IT infrastructure from procurement to end-of-life. AM facilitates enterprise management of physical objects and the events associated with the life cycle of these objects. CIT is integrated with AM to assist in importing data to the AM database.

Developer/manufacturer: Hewlett-Packard Enterprise Development L.P.

Documentary evidences developed by Corsec Security, Inc.

Sponsor: Hewlett-Packard Enterprise Development L.P.

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

ITSEF: Epoche & Espri S.L.U.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL2+ (ALC_FLR.2).

Evaluation end date: 30/12/2015.

All the assurance components required by the evaluation level EAL2+ (augmented with ALC_FLR.2 Flaw reporting procedures) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product “HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)”, a positive resolution is proposed.

TOE summary

The TOE is a software-only TOE and provides an organized way to manage the life cycle of IT infrastructure from procurement to end-of-life. AM facilitates enterprise management of physical objects and the events associated with the life cycle of these objects. CIT is integrated with AM to assist in importing data to the AM database.

AM provides organizations with visibility into their current IT hardware and software inventories, as well as non-IT assets such as office supplies, machines, and tools.

AM provides insights into the current status of assets, such as contracts, licensing obligations, and when software is over-deployed for an environment. Assets are organized within AM into portfolio items, which contain a list of assets, information relevant to who is responsible for the assets, and where the assets are located geographically.

Connect-It is embedded in AM to assist in importing asset data from external discovery tools. Connect-It not only feeds various types of data into AM, but also pushes asset data to external service management, configuration management, cloud services, and other corporate systems.

TOE major security features

The major security features implemented by the TOE and subject to evaluation (no assurance can be supposed to any other functionality) to can be summarised as follows:

- Cryptographic Support: the TOE provides two FIPS 140-2 validated cryptographic libraries that provide cryptographic services for the TOE. All keys are generated according to FIPS standards for key generation and destroyed via FIPS-approved zeroization methods. Cryptographic operations are provided to secure communications among various physically-separated TOE components and trusted IT products in the TOE environment. Secure operations use TLS v1.1 or v1.2 in the evaluated configuration.
- User Data Protection: the TOE implements role-based access controls on all users attempting to access the various screens of the AM UIs, the data stored in the AM database, and all connectors attempting to import data to or export data from the TOE. By default, all users with accounts on the TOE are given a set of guest permissions that can be modified by a user with Administrative rights permissions. Users with Administrative rights permissions can also give a different set of permissions to each user.
- Identification and Authentication: the Connect-It client allows users to create and manage scenarios and connections to external discovery and inventory tools prior to identification and authentication. For all other functions, the TOE requires users to authenticate before granting access to functionality or data within the TOE. While authenticating, the TOE obscures user passwords by replacing the individual characters with bullets while the user is typing the password at the login prompt. The TOE supports the use of certificates or LDAP for authentication. User accounts can be configured to be locked out after a user with Administrative rights permissions-configurable number of failed login attempts.

- Security Management: the TOE is managed primarily via the AM and Connect-It UIs. All user accounts have an "Administration Rights" permission which can be enabled by authorized users with Administrative rights permissions to grant full access to the functionality of these interfaces and all data in the database. Otherwise, access is constrained by a highly customizable role-based access control system. Management tasks available to users with Administrative rights permissions include management of license keys, databases, and user roles and permissions.
- Protection of the TSF: the TOE provides a secure connection to a remote LDAP server that is used whenever credentials are passed to be evaluated. The TOE performs cryptographic self-tests during startup to test the proper function of the cryptographic modules. The TOE also performs conditional self-tests during the operation of the cryptographic module in order to ensure that critical functionality of the cryptographic module is working properly.
- Trusted Path/Channels: the TOE provides a trusted path between users accessing the TOE via the AM web UI. This path uses TLS and its supported cryptographic functionality to secure all communications between the user workstation and the Tomcat server running on the server components of the TOE.
- Asset Management Analysis: once data is imported or input into AM, the data can be analyzed to ensure that only authorized users have access to assets and that authorized hardware and software is being used with an asset.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2 Flaw reporting procedures, according to Common Criteria v3.1 R4.

Class	**Family/Component**
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 ASE_TSS.1 TOE summary specification
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification

	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_COV.1 Evidence of coverage 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 R4:

Class	Family/Component

FCS	FCS_CKM.1
	FCS_CKM.4
	FCS_COP.1(a)
	FCS_COP.1(b)

FDP	FDP_ACC.1 FDP_ACF.1 FDP_ETC.2 FDP_ITC.1
FIA	FIA_AFL.1 FIA_UAU.1 FIA_UAU.5 FIA_UAU.7 FIA_UID.1
FMT	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1
FPT	FPT_ITC.1 FPT_TST.1
FTP	FTP_TRP.1
AMA_SAA.1	
AMA_SAD.1	

IDENTIFICATION

Product: “HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)”

Security Target: Hewlett-Packard Enterprise Development L.P. Asset Manager v9.50 with Connect-It v9.60 Security Target, v 1.4

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL2+ (ALC_FLR.2).

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

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 [ST]. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

- A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.
- A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
- A.LOCATE The TOE and external database are located within a controlled access facility.
- A.PROTECT The TOE software will be protected from unauthorized modification.
- A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- A.NOEVIL The users with Administrative rights who manage the TOE and database administrators who manage the TOE environmental components are non-hostile, appropriately trained, and follow all guidance.

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment are listed below. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a basic skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE. An attacker may initiate a process within the TOE to act on its behalf. This process is assumed to have all attributes of the attacker.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and no physical access to the TOE. TOE users only have access to the TOE remotely.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. The threats defined are:

- T.MASQUERADE An attacker or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
- T.TAMPERING An attacker or process may be able to bypass the TOE’s security mechanisms by tampering with the TOE or TOE environment.
- T.UNAUTH An attacker or a TOE user may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.
- T.FALREC Attackers may use the TOE to order or install unauthorized items on the network.
- T.INTERCEPT The TOE may communicate with remote IT entities and user workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.

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.

IT Security Objectives that are to be satisfied by the environment:

- OE.PROTECT: the TOE environment must protect itself and the TOE from external interference or tampering.

- OE.PLATFORM: the TOE hardware and OS must support all required TOE functions.
- OE.ACCESSIBILITY: the TOE is positioned on the network such that authorized users are able to access the TOEs functionality while unauthorized external users are blocked from accessing the TOE.

Non-IT Security Objectives that are to be satisfied without imposing technical requirements on the TOE:

- OE.MANAGE: sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.
- OE.PHYSICAL: the physical environment must be suitable for supporting a computing device in a secure setting.

ARCHITECTURE

LOGICAL ARCHITECTURE

The software-only TOE is a resource tracking tool which provides an organized way to manage the life cycle of IT infrastructure from procurement to end-of-life.

The TOE is deployed on three platforms. The platforms are part of the TOE environment, but the TOE components on each platform are described below:

- Client:
  - AM Client provides user interface and CLI utilities for AM.
  - Connect-It Client provides user interface and CLI utilities for Connect-It and all Connect-It functionality.
  - OpenSSL FIPS module provides secure communications for the Client
- AM Front End Server:
  - AM Web Tier provides web-based access for non-client users.
  - Apache Tomcat server hosts the web interfaces.
  - BSAFE Crypto-J FIPS module provides secure communications for Front End Server.
- AM Back End Server:
  - AM API provides access to database and accepts connections from AM Front End and external components.
  - Apache Tomcat server hosts the web interfaces.

- BSAFE Crypto-J FIPS module provides secure communications for Back End Server.
- AM Server Components includes Asset Portfolio, Procurement, Contracts, Financials, and Software Asset Management as described above.

The BSAFE Crypto-J FIPS libraries and OpenSSL FIPS library provide the TOE with the capability to generate and destroy keys and perform cryptographic operations. These operations include secure communications between some TOE components, secure management on the AM web UI, and secure communications with a LDAP server. These libraries also perform start-up self tests to verify cryptographic functions prior to offering these functions.

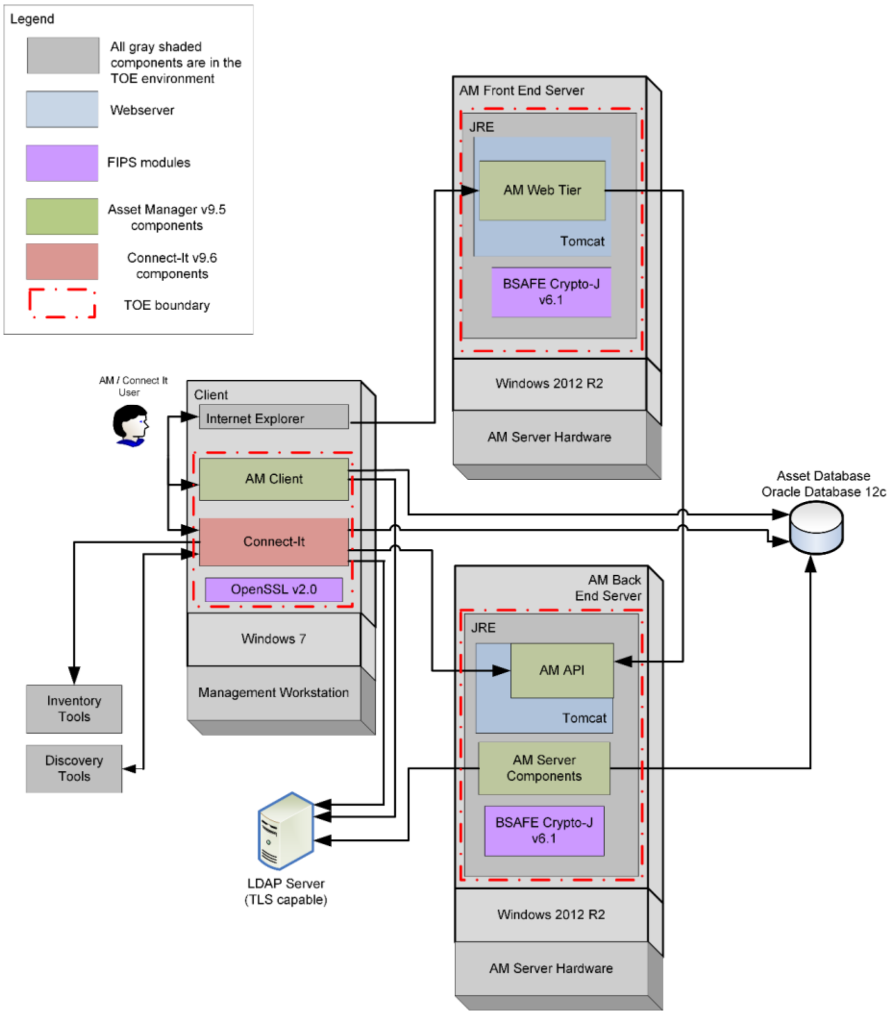
The Connect-It client allows users to create and manage scenarios and connections to external discovery and inventory tools prior to identification and authentication. For all other functions, the TOE requires user to authenticate before granting access to functionality or data within the TOE. During authentication the TOE obscures user passwords with bullets. After authentication, the TOE implements role-based access controls for user attempting to access the various screens of the AM UI, the data stored in the AM database, and all connectors attempting to import data to or export data from the TOE. By default, users are given a set of guest permissions that can be modified by a user with Administrative rights permission. A user with Administrative rights permissions can configure user accounts to lock out users after a configurable number of failed login attempts.

The AM and Connect-It UIs are the primary management interfaces for the TOE. Users with Administrative rights permissions are granted full access to the functionality of these interfaces and all data in the database. Other users have access restricted according their role-based access control settings. Administrative rights permissions allow a user to manage license keys, databases, database objects, and user roles and permissions.

Data stored within the AM database can be analyzed to ensure that only authorized users have access to assets and that only authorized hardware and software is used by an asset.

PHYSICAL ARCHITECTURE

The next figure illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.



The TOE is a resource tracking tool which runs on a Windows or Linux Operating System (OS). The TOE is software only is delivered via the HP download site https://softwaresupport.hp.com/. The TOE is installed on a client and two server platforms as depicted in the previous figure. The essential physical components of the TOE in the evaluated configuration are

- Asset Manager v9.50 software
- Connect-It v9.60 software
- Server to host the Asset Manager software,

DOCUMENTS

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

- HP Asset Manager Software Version: 9.50 Installation and Upgrade
- HP Asset Manager Software Version: 9.50 Administration
- HP Asset Manager Software Version: 9.50 Concepts and Implementation
- HP Asset Manager Software Version: 9.50 Programmer Reference
- HP Asset Manager Software Version: 9.50 User Interface
- HP Asset Manager Software Version: 9.50 Release Notes
- HP Asset Manager Software Version: 9.50 Web Implementation
- HP Connect-It Software Version: 9.60 Quick Start
- HP Connect-It Software Version: 9.60 User Guide
- HP Connect-It Software Version: 9.60 Connector Guide
- HP Connect-It Software Version: 9.60 Asset Manager Database Integration Solution
- HP Connect-It Software Version: 9.60 Programmer’s Reference
- HP Connect-It Software Version: 9.60 Release Notes

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the security target [ST].

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 TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST]. The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in security target [ST].

PENETRATION TESTING

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 TOE does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

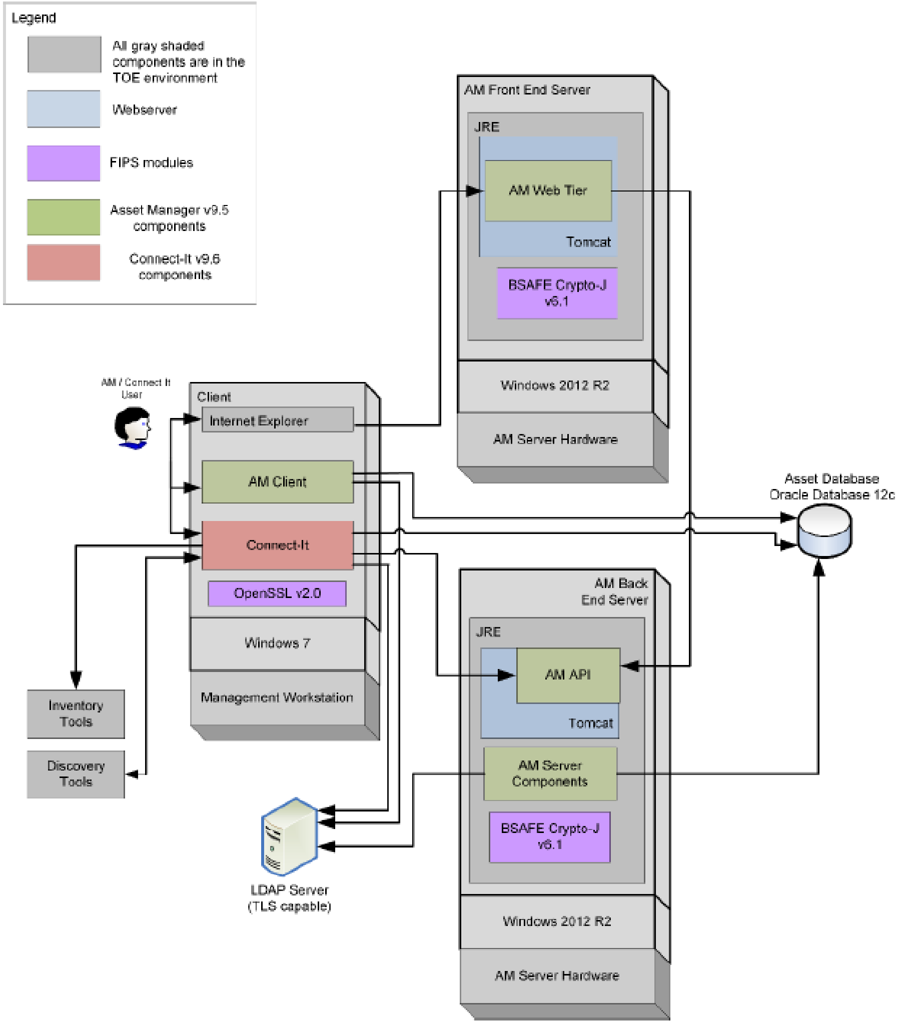
EVALUATED CONFIGURATION

The TOE is defined by its name and version number:

- HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)

To set up the TOE in a way consistent to the evaluated configuration and the operational environment defined in the security target [ST], users must follow the steps included in the installation and operation manuals (see section DOCUMENTS).

The deployed configuration for the evaluation is presented in the following figure:



EVALUATION RESULTS

The product "HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)" has been evaluated against the "Hewlett-Packard Enterprise Development L.P. Asset Manager v9.50 with Connect-It v9.60 Security Target, v 1.4"

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

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

- The fulfilment of the assumptions within indicated in the security target [ST] is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- It is very important the adequate fulfilling of the installation procedures; the installation procedure may be vulnerable if those procedures are not followed.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product "HP Asset Manager v9.50 with Connect-It v9.60 version build #12154 (AM) and 010 (CIT)", a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ST] Hewlett-Packard Enterprise Development L.P. Asset Manager v9.50 with Connect-It v9.60 Security Target, v 1.4

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Hewlett-Packard Enterprise Development L.P. Asset Manager v9.50 with Connect-It v9.60 Security Target, v 1.4.