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

REF: 2009-27-INF-754 v1	Created: CERT3
Distribution: Public	Reviewed: CALIDAD
Date: 20.10.2011	Approved: TECNICO

CERTIFICATION REPORT

Dossier: 2009-27 HERMES-PI3 v1.0

Applicant Data: S2800109G SECRETARÍA DE ESTADO DE SEGURIDAD

References:

[EXT868] Certification Request of HERMES-PI3 v1.0

[EXT1452] IEvaluation Technical Report of HERMES-PI3 v1.0, Epoche & Espri.

Certification Report of HERMES-PI3 v1.0, as requested by Secretaría de Estado de Seguridad in [EXT-868], dated 11/12/2009, and evaluated by the laboratory EPOCHE & ESPRI, as detailed in the Evaluation Technical Report [EXT-1452], received on 23/09/2011.

TABLE OF CONTENTS

SUMMARY

This document constitutes the Certification Report for the product HERMES-PI3 v1.0.

Developer/manufacturer: INDRA Sistemas S.A.

Sponsor: Centro Nacional de Protección de Infraestructuras Críticas (CNPIC); Secretaría de Estado de Seguridad-Ministerio del Interior.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: EPOCHE & ESPRI.

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R3 – EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1).

Evaluation end date: 22/09/2011.

All the assurance components required by the level EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1) 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 EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1) methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM]. Considering the obtained evidences during the instruction of the certification request of the HERMES-PI3 v1.0, a positive resolution is proposed.

TOE SUMMARY

HERMES is an IT system which purpose is to manage the information related to national critical infrastructures (referred from now on as CI data), allowing the collaboration among the different agents in charge of the management and protection of such infrastructures.

HERMES consists of two platforms, named HERMES-PI3 and HERMES-ARGOS and the corresponding data bases. The Target of Evaluation (TOE) considered by the present document relates to HERMES-PI3 only. The TOE is a Web application that implements the functionality for the management of the CI data. CI data is securely stored in a data base which is outside the TOE boundaries.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1) in accordance with ([CC-P3]).

Assurance Class	Assurance Components
Security Target Evaluation	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
Development	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
Guidance	AGD_OPE.1, AGD_PRE.1
Life Cycle	ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_TAT.1
Tests	ATE_COV.1, ATE_FUN.1, ATE_IND.2
Vulnerability Analysis	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies several requirements as stated by its Security Target, in accordance with ([CC-P2]).

- FAU_GEN.1 - Audit data generation
- FAU_GEN.2 - User identity association
- FAU_SAR.1 - Audit review
- FAU_SAR.2 - Restricted audit review
- FAU_SAR.3 - Selectable audit review
- FDP_ACC.1 - Subset access control
- FDP_ACF.1 - Security attribute based access control
- FDP_ETC.1 - Export of user data without security attributes
- FIA_AFL.1 - Authentication failure handling
- FIA_ATD.1 - User attribute definition
- FIA_SOS.1 - Verification of secrets
- FIA_SOS.2 - TSF Generation of secrets
- FIA_UAU.2 - User authentication before any action
- FIA_UAU.5 - Multiple authentication mechanisms
- FIA_UAU.6 - Re-authenticating
- FIA_UID.2 - User identification before any action
- FIA_USB.1 - User-subject binding
- FMT_MSA.1 RBAC - Management of security attributes (Role-based Access Control)

- FMT_MSA.1 PI3AC - Management of security attributes (PI3 Access Control)
- FMT_MSA.3 RBAC - Static attribute initialisation (Role-based Access Control)
- FMT_MSA.3 PI3AC - Static attribute initialisation (PI3 Access Control)
- FMT_MTD.1 - Management of TSF data
- FMT_MTD.2 - Management of limits on TSF data
- FMT_REV.1 - Revocation
- FMT_SAE.1 - Time-limited authorisation
- FMT_SMF.1 - Specification of Management Functions
- FMT_SMR.1 - Security roles

Additionally, the following extended components have been defined:

- FCS_CKM.5 - Delegated cryptographic key derivation
- FCS_COP.2 - Delegated cryptographic operation
- FDP_ACC.3 - Delegated complete access control
- FDP_ACF.2 - Delegated security attribute based access control

IDENTIFICATION

Product: HERMES-PI3 v1.0.

Security Target: HERMES-PI3 Security Target EAL2+, v1.6, 22th July 2011.

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R3 – EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1).

SECURITY POLICIES

The usage of HERMES-PI3 v1.0 implies to implement a series of organizacional policies that assure the commitment of different demands of security.

The details about them are included in the Security Target. In synthesis, the necessity settles down to implement organizational policies relative to the following matters.

OSP.USAGE. The information provided by the TOE and accessed by the authorised users will only be used for authorised purposes.

OSP.MANUAL. The users follow the TOE manuals for the secure administration of the TOE, the synchronization process, the audit functions, and the daily operations they may perform.

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.

ASSUMPTIONS ON THE OPERATIONAL ENVIRONMENT

AS.TERMINAL. It is assumed that the terminal from which a user accesses the TOE is correctly protected and implements security measures that avoid, among other types of attacks, session hijacking.

AS.PLATFORM. It is assumed that the platform where the TOE is installed and operated is free from any malware that could subvert the TSF and thus compromise the confidentiality of the assets, that the necessary underlying security measures (e.g. antivirus, IDS, etc.) that prevent the platform from being infected are periodically updated and checked, and that the clock of the server is accurately set.

AS.DB. It is assumed that the Data Base where the CI Data is stored implements integrity and confidentiality assurance mechanisms that prevent the CI Data from being modified by or disclosed to an unauthorised user.

AS.PHYSICAL. It is assumed that the physical platform and data centre where the TOE is installed and operated is protected by appropriate physical security measures (e.g. access control, surveillance cameras, etc.) to ensure that only authorised personnel are allowed access.

AS.NETWORK. It is assumed that the TOE is not connected to untrusted networks, and if it does, there are appropriate network elements (e.g. Reverse proxy) that permit establishing a protected channel between the users and the TOE (e.g. VPN).

AS.GIS. It is assumed that the Geographical Information System (GIS) to which the TOE connects for the retrieval of the geographical maps is a trusted entity, and the connection is established using a secure channel (i.e. SSL channel). The GIS maps are used by the TOE along with CI geospatial data (Block E) to allow an authorized user to accurately locate the critical infrastructures.

ASSUMPTIONS ON THE TOE PERSONNEL

AS.PERSONNEL. It is assumed that TOE users holding the privilege “Execution of platform synchronization”, that grants the capability to perform the synchronization of CI data (export), and/or the privilege “Management of System security attributes”, that grants the capability to manage the security attributes of the TOE, including user accounts, roles, and system security configuration (i.e. password quality metrics and management metrics), behave according to what it is expected, and do not act in a malicious manner.

THREATS

This section shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two. So the following threats are not an exploitable risk for the system, always under the assumptions and security policies listed. For any threat not included in this list the result of the evaluation, nor the corresponding certificate, guarantee any resistance.

T.ACCESS. An attacker attempts to access TOE resources for which she is not authorised by impersonating a legitimate user with such privileges. This threat covers the online threat carried out by either an authenticated user or an external agent.

T.SYN. An unauthorised user attempts to gain access to the information stored in the portable storage device during a synchronization process, or afterwards (e. g. The device is not properly zeroized or destroyed). This threat covers the offline threat carried out by an external agent.

OPERATIONAL ENVIRONMENT OBJECTIVES

The system requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the 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.ACCESS. The environment shall implement a role-based access control policy in a manner that the TOE is able to delegate the authorization procedure once the user is correctly authenticated. This access control policy shall assure that users have access only to the authorised resources and can perform the authorised actions on those resources.

OE.SYN. The environment shall encrypt the CI Data to be synchronized before the export is carried out and decrypt the encrypted CI Data after the import. The environment shall follow the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode and using a 256-bit length key. The environment shall add a mandatory PKCS#5 padding to each file to be encrypted. The environment shall follow the Password-based Key Derivation Function 2 (PBKDF2), as described in PKCS#5 standard, for the encryption/decryption key derivation. The password shall be requested to the operator, and the initialization vector (IV), salt and counter shall be dynamically generated at export, and retrieved at import. As a result, the environment shall store in the portable storage device the initialization vector (IV), the salt and counter used during the encryption.

OE.DESTRUCTION. The environment shall securely destroy the portable storage device or the information therein contained in order to avoid an attacker gain access to the CI Data.

OE.TERMINAL. The terminal from which a user accesses the TOE shall be correctly protected and implement security measures that avoid, among other types of attacks, session hijacking.

OE.PLATFORM. The platform where the TOE is installed and operated shall be free from any malware the underlying security measures (e.g. antivirus, IDS, etc.) to prevent the platform from being infected are periodically updated and checked, and the clock of the server is accurately set.

OE.BD. The Data Base that stores the CI Data shall implement integrity and confidentiality assurance mechanisms that prevent the CI Data from being modified by or disclosed to an unauthorised user.

OE.PHYSICAL. The physical platform and data centre where the TOE is installed and operated shall be protected by appropriate physical security measures (e.g. access control, surveillance cameras, etc.) to ensure that only authorised personnel are allowed access.

OE.NETWORK. The environment where the TOE is operating shall provide the necessary network elements to ensure a protected channel between users connecting from an untrusted network (e.g. Internet) and the TOE.

OE.GIS. The Geographical Information System (GIS) to which the TOE connects for the retrieval of the geographical maps shall be a trusted entity, and the connection shall be established using a secure channel (i.e. SSL channel). The GIS maps are used by the TOE along with CI geospatial data (Block E) to allow an authorized user to accurately locate the critical infrastructures.

OE.PERSONNEL. The TOE users holding the privilege “Execution of platform synchronization” and/or the privilege “Management of System security attributes” shall behave according to what it is expected, and shall not act in a malicious manner. In addition, TOE users holding the privilege “Execution of platform synchronization”, and/or that will manage the portable storage device used in a synchronization, shall prevent unauthorised entities from accessing the information contained in such device.

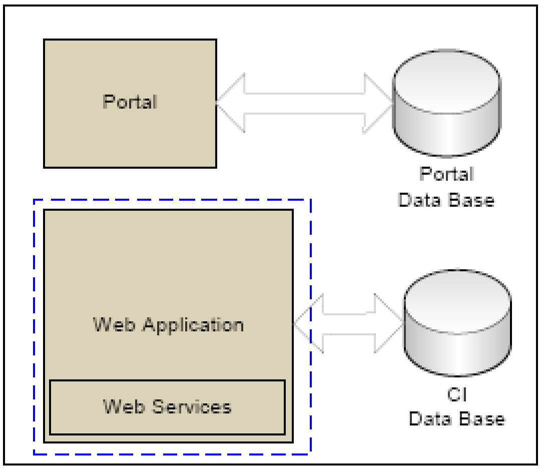
OE.USAGE. The information provided by the TOE and accessed by the authorised users shall only be used for authorised purposes.

OE.MANUAL. The users shall follow the TOE manuals for the secure administration of the TOE, the synchronization process, the audit functions, and the daily operations they may perform.

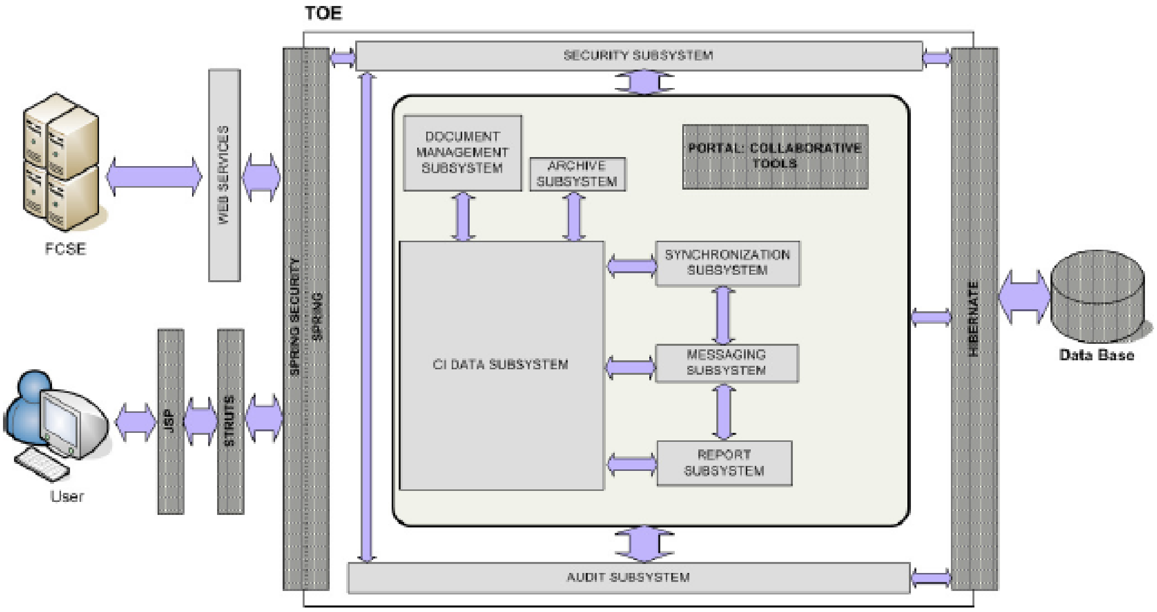
TOE ARCHITECTURE

LOGICAL ARCHITECTURE

The next Figure shows the overview of TOE logical Boundary:



The Web Application architecture is detailed in the next figure:



Security Subsystem

This subsystem provides a holistic and horizontal service for the TOE, and affects the rest of the subsystems.

The Security subsystem implements the password-based and X.509 certificate-based authentication mechanisms, and ensures that every user is correctly authenticated before the access control policies are enforced. In particular, the

RBAC Policy is delegated to Spring Security Framework, while the PI3AC Policy is implemented by this Subsystem.

The validation of X.509 certificates is completed invoking the validation service configured for the Certification Authority that issued the user's certificate, and which is managed by the Subsystem itself.

Additionally, this Subsystem offers the security administrators a wide range of management functionalities to configure the users' accounts and roles, as well as the security attributes of the TOE.

Audit Subsystem

This subsystem is in charge of recording every event that may be of interest for auditing purposes. As it receives input from every subsystem, it is considered a horizontal service as well.

CI Data Subsystem

This subsystem is the core of the TOE, and is in charge of managing the information related to the critical infrastructures (CI Data).

Document Management Subsystem

This subsystem implements document management functionalities for those documents that may be uploaded by the system users.

Archive Subsystem

This subsystem is responsible for archiving the information that the system has ever managed, even though the information is no longer active in the system. It permits to retrieve old information if necessary.

Synchronization Subsystem

This subsystem implements the export and a wrapper of the cryptographic operations (key derivation, encryption and key destruction) that allow an operator to further synchronize updated or new CI into HERMES-ARGOS. In particular, the key derivation and encryption operation are delegated to the environment.

Message Subsystem

This subsystem notifies certain users of the system respecting a customized set of events (e.g. when a new CI is created after a synchronization procedure, when an already existent CI is modified by an operator, etc.).

Report Subsystem

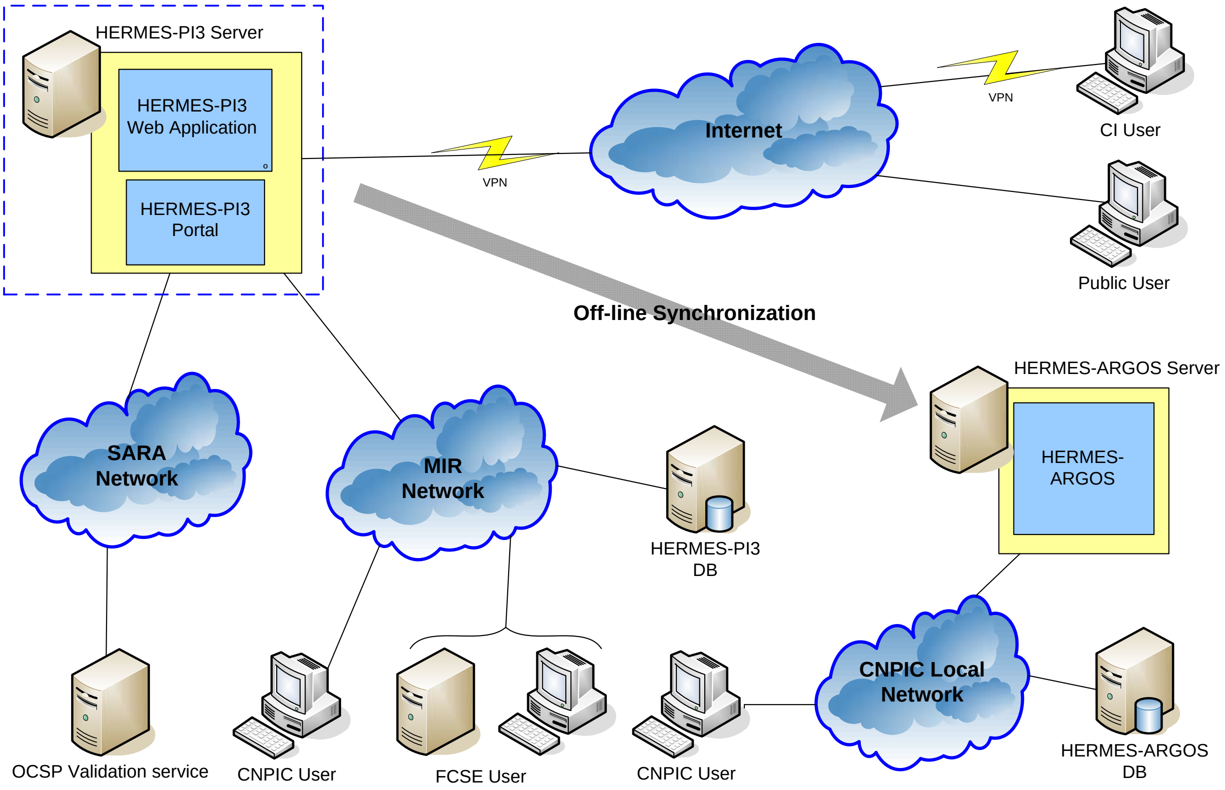
This subsystem permits an operator to generate reports containing filtered information, like CIs that belong to a certain enterprise.

Web Services Subsystem

The Web Services Subsystem has been designed to allow external applications to retrieve critical infrastructures information in a secure C2B fashion. The TOE publishes a series of web services that can be accessed by authorised users. These services follow a request-response protocol based on SOAP messages, allowing users to request information of specific critical infrastructures. Security measures for protecting SOAP messages are delegated to the Security Subsystem.

PHYSICAL ARCHITECTURE

Next figure shows the TOE physical boundary.



In the HERMES- PI3 Server, two elements are therein included: HERMES-PI3 Web Application and HERMES-PI3 Portal. The TOE is limited to HERMES-PI3 Web Application, not including HERMES-PI3 Portal. The server stores the information (CI Data) in an external Data Base (HERMES-PI3 DB), which is not part of the TOE and thus is considered to be part of the Operational Environment.

Therefore, the TOE does not include any hardware or firmware.

DOCUMENTS

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

- HERMES - Manual de Instalación, Configuración y Mantenimiento
- HERMES - Manual de Sincronización
- HERMES - Política de Seguridad Administrador

- HERMES - Política de Seguridad Usuario
- HERMES PI3 - Manual de Administrador
- HERMES PI3 - Manual de Usuario

TOE TESTING

The TOE configuration under testing is consistent to the version defined in the Security Target (ST).

The developer has tested all security functions and the evaluator has successfully checked the tests carried out by the developer. The evaluator implemented the test plan with all the information needed to reproduce each test.

Additionally, the evaluator has carried out a set of independent tests, in accordance with the evidence from the developer tests. The independent tests were successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

Therefore, testing has been done in such a way that the security functionality was completely tested.

TOE CONFIGURATION

Following software requirements are needed for installing and operating HERMES-PI3:

- Linux Red Hat Enterprise 5.
- Oracle Database 10g Release 2 (10.2.0.1.0) Enterprise/Standard Edition for Linux x86.
- Oracle Database Family: Patchset 10.2.0.4.0 Patch set for Oracle database server (Patch 681089).
- Java JDK/JRE 1.6 or higher.
- JBOSS 4.2.3 or higher.
- Hibernate v3.2.
- J2EE Spring Framework v2.5.6 and Spring Security v2.0.5.
- Security Patch SpringSource Spring Framework 2.5.6.SEC02.
- J2EE Struts Framework v2.1.8.
- Spring Web Services 1.5.6.

Following hardware requirements are needed for installing and operating HERMES-PI3:

- Solaris server 9 with a 2 GHz or higher processor and 4 GB RAM or more.
- Hard disk 500 GB.

Following requirements are needed for accessing the Web application deployed in HERMES-PI3 from a Personal Computer (PC):

- A standard PC with a 1GHz or higher processor and 1GB RAM or more
- Microsoft Windows XP/2000
- Internet Explorer v7 or higher or Mozilla Firefox v3.0 or higher
- Java JRE 1.6
- Internet connection

EVALUATION RESULTS

All evaluation activities have a PASS verdict. Therefore, the evaluator has assigned a PASS verdict to the evaluation of product HERMES-PI3 v1.0.

The TOE HERMES-PI3 v1.0, satisfies its Security Target "HERMES-PI3 Security Target EAL2+, v1.6, 22th July 2011", according to CC 3.1 R3 and CEM 3.1 R3, EAL2+ (ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1).

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The following recommendations to the users of HERMES-PI3 v1.0 are highlighted as the result of the evaluation process:

- The installation process must be accurately followed and every requirement established by the installation and hardening manual of the operating system used by the TOE must be met.

- The application server and data base versions must be those established by the TOE documentation in order to avoid the vulnerabilities found in former versions.

- Certificates used by the TOE for users authentication and web services use must come from a trusted PKI.

- The connection used for the geographic positioning system, with Google Maps API, must be implemented by SSL. By this way, the confidentiality of CI data is ensured.

- Users must be previously trained in order to comply with TOE operating manuals.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product HERMES-PI3 v1.0, a positive resolution is proposed.

GLOSSARY

CI	Critical Infrastructures
CC	Common Criteria
CCN	Centro Criptológico Nacional
CEM	Common Evaluation Methodology
CNI	Centro Nacional de Inteligencia
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GIS	Geographical Information System
IT	Information Technology
OC	Organismo de Certificación
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality

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

It is available, jointly with this Certification Report, the security target of HERMES-PI3 v1.0: “HERMES-PI3 Security Target EAL2+, v1.6, 22th July 2011”.