CNPIC

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN SOBRE INFRAESTRUCTURAS (HERMES –PI3)

SECURITY TARGET

EAL2+

Π③

Table of Contents

Date	Ver./Rev.	Description	
28/10/2009	**1.0**	Start Edition.	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.
		Review by:	**Date**
		Miguel Ángel Abad Arranz Centro Nacional de Protección Infraestructuras Críticas (CNPIC)	04/11/2009
29/03/2010	**1.1**	Update Edition.	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	15/04/2010
21/04/2010	**1.2**	Update Edition.	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	04/05/2010
13/10/2010	**1.3**	Update Edition (Introduction section, including privileges and roles matrix)	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	10/11/2010
29/11/2010	**1.4**	Updated OE.PERSONNEL and related rationale.	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	14/12/2010
07/06/2011	**1.5**	Assumption AS.GIS added to the operational environment.	
		Author:	Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.

Date	Ver./Rev.	Description	
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	22/07/2011
22/07/2011	**1.6**	Deleted Contact from Ministry as TOE role	
		Author: Jorge López Hernández-Ardieta Security Division, INDRA Sistemas S.A.	
		Review by:	**Date**
		Jose Emilio Rico Epoche & Espri Laboratory	22/07/2011

DISTRIBUTION AND APPROVAL HISTORY

Addressee	Ver. /Rev.	Number of Copies	Distribution Page Code and Date
Name and or Position and Organization.	Nº	Nº	

Introduction

ST reference

1 **Title:** HERMES-PI3 Security Target EAL2+

2 **Version:** 1.6

3 **Author:** INDRA Sistemas S.A.

4 **Publication date:** 22nd July 2011

TOE reference

5 HERMES-PI3, version 1.0

TOE overview

TOE usage and major security features

6 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.

7 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.

8 Both platforms have been designed following the same approach and implementing the same application-level security mechanisms. However, the level of classification of the information managed by each one differs. HERMES-ARGOS is devised to manage more sensible information than HERMES-PI3, and therefore the access to it is restricted to users belonging to the CNPIC (*Centro Nacional de Protección de Infraestructuras Críticas*). On the other hand, users that have access to HERMES-PI3 Platform include the CNPIC, the Spanish Security Corps and Forces (FCSE, *Fuerzas y Cuerpos de Seguridad del Estado*) and the assigned stakeholders of the CI. As a result, there is a physical and logical separation between the boundaries of the Platforms.

9 Due to this architectural constraint, and because both platforms share certain blocks of CI data (see section TOE Description), a robust and secure unidirectional synchronization mechanism has been implemented. The synchronization procedure is performed by means of an air-gap method. The data to be synchronized is

encrypted and stored in a Read-Only portable storage device (e.g. CD-R) using the export operation implemented in HERMES-PI3 platform. On the other hand, the import is carried out into HERMES-ARGOS platform, which implements the decryption operation.

10 The next Figure 1 depicts the synchronization procedure.

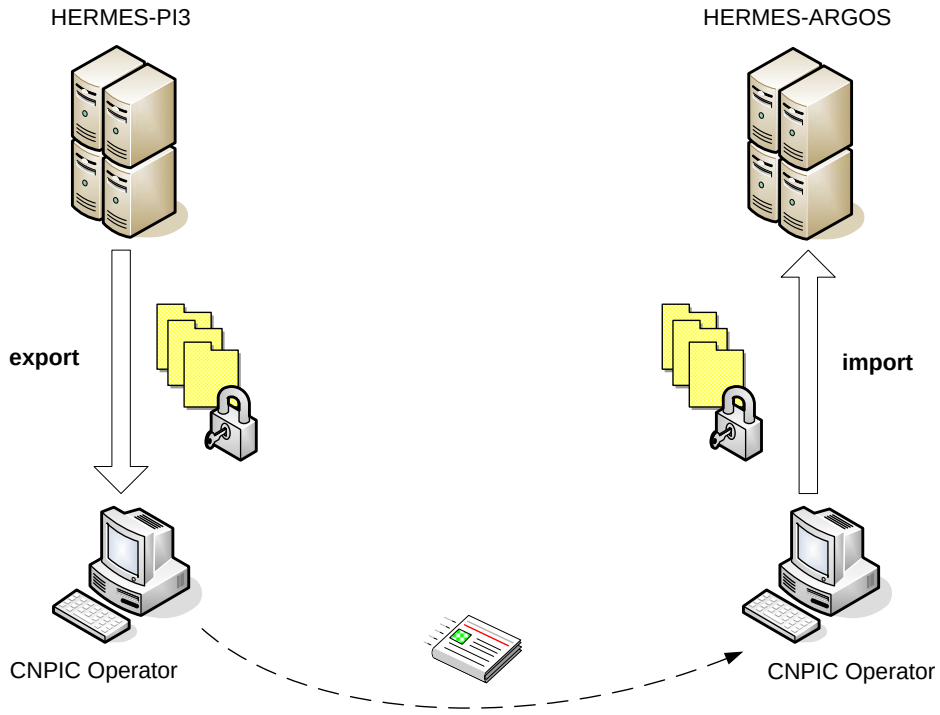


Figure 1 Synchronization process

11 HERMES uses an implementation of the Advanced Encryption Standard (AES) algorithm in CBC mode, with a key length of 256 bits. Both Platforms also implement a Key Derivation Function where the encryption / decryption keys are derived from a password provided by the CNPIC operator during the export / import procedures, respectively.

12 A signed Java Applet is downloaded to the CNPIC Operator computer in order to perform the synchronization process. The Applet allows the operator to select the CI information (files) to be exported, requesting a synchronization password which will be later used during the import. Once encrypted, the CI information is sent by the TOE to the Applet along with the parameters used in the cryptographic

operations: password, initialization vector IV, counter and salt – see TOE description below for further information about these items.

13 The TOE internally delegates the environment to encrypt the information before sending it to the Applet in the export operation. The encryption key is derived by the environment using the password provided by the operator, and the dynamically generated initialization vector IV, counter and salt. The Applet is outside the scope of the TOE. Notwithstanding, it should be mentioned that the CI data (files) that will be managed by the Applet is always kept encrypted.

14 Access to the TOE functionality is protected by means of a fine-grained **Role-based Access Control mechanism** (RBAC) provided by the environment, and thus not implemented by the TOE. On the other hand, the **PI3 Access Control Policy** (PI3AC), implemented by the TOE, is also applied every time access to CI Data is requested. RBAC Policy is always enforced, independently of the resource or action requested by the user. PI3AC Policy is applied afterwards if the requested resource corresponds to CI Data, offering a second level of access control. In this case, PI3AC will restrict the critical infrastructures, and fields of data of each one, that the user can access to.

15 Exceptionally, access to the synchronization capability – where CI Data is managed – is only protected by the RBAC Policy in order to allow the export of all the information of the CI Data that needs to be synchronized. In any case, the user is not able to access the plain text of the CI Data since it is encrypted before leaving the TOE.

16 Moreover, the TOE implements the authentication mechanism, which is always enforced before the RBAC and PI3AC policies are applied. Two authentication methods are supported by the TOE: password-based and X.509 certificate-based.

17 The operations a user can perform depend upon a correct authentication and a correct authorisation. Depending on the operation and information requested, either RBAC or both RBAC and PI3AC Policies are enforced. In RBAC Policy, the authorisation depends upon the matching between the privileges inherited from the role(s) of the authenticated user and the privileges required for the particular operation. In PI3AC Policy, the authorisation depends upon the visibility conditions and infrastructures associated for the authenticated user. See TOE description below for further information.

18 The TOE also implements an audit system that records every action made during the operation of the platform.

TOE type

19 The TOE is a Web application to allow the users involved in the protection and management of the Spanish Critical Infrastructures to share related information amongst them. It comprises the application logic and the security functions such as

the users' identification and authentication, users' authorization by means of PI3 Access Control Policy, management of roles and security attributes, and audit.

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

20 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.

21 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.

22 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

TOE description

23 This section provides a detailed description about the TOE components, boundaries and security measures implemented.

Information managed by the TOE

24 The information managed by HERMES is CLASSIFIED, and the level of classification differs between HERMES-PI3 and HERMES-ARGOS. There are five levels of classification defined by the Spanish Government, which are, quoted from highest to lowest level of security: SECRET (*SECRETO*), RESERVED (*RESERVADO*), CONFIDENTIAL (*CONFIDENCIAL*), LIMITED DISSEMINATION (*DIFUSIÓN LIMITADA*) and NON-CLASSIFFIED (*SIN CLASIFICAR*).

25 In particular, HERMES-PI3 manages information (CI data) classified as LIMITED DISSEMINATION inside HERMES-PI3 operation boundaries. As a result, access to the CI data is restricted to only certain users, in particular, CNPIC staff, FCSE staff and CI stakeholders.

26 In HERMES, the information is split into six different blocks. Each platform (HERMES-PI3 and HERMES-ARGOS) manages a subset of those blocks of information. Next table indicates the existent blocks of information as well as the blocks accessible by each platform.

Block of Information	HERMES-ARGOS	HERMES-PI3
Block A: General Data	X	X
Block B: Security Data	X	X
Block C: Localization Data	X	X
Block D: Strategic Data	X	
Block E: Archives	X	
Block F: GIS Data		X

Table 1 Blocks of Information in HERMES

Access Control Policies

27 This part describes the *Role-Based Access Control Policy* implemented by the Environment and the *PI3 Access Control Policy* implemented by the TOE. The combination of both provides a complete access control of the TOE users.

Role-Based Access Control Policy (RBAC): Roles of the TOE users and privileges

28 The TOE delegates the environment to enforce an access control mechanism. In particular, the delegated access control is implemented by *Spring Security Framework (SSF)*, which provides a *Role-Based Access Control Policy* (RBAC Policy) that assures that only authorised users have access to and perform the corresponding authorised operations on the CI data.

29 In order to allow SSF to correctly enforce the RBAC Policy, the TOE implements the management functionality for associating users to Roles, and Roles to a set of allowed operations and privileges. *SSF* will then restrict the access to the protected resources not only by filtering the Web resources that a Role has access to but also by restricting the operations (actions) that the Role can perform on that Web resource. The RBAC Policy is enforced on authenticated users. Consequently, the environment obtains certainty about the roles and privileges bound to the particular subject and that must be used for the authorization.

30 Next privileges have been established for the TOE:

Privilege	Description
(1) Access to collaborative tools [Consulta del portal colaborativas]	Grants access to the Forum and Wiki collaborative tools of the TOE.
(2) Access to CI data [Consulta de datos del catálogo]	Grants access to the CI data of the TOE, in accordance with visibility conditions and the explicitly permitted critical infrastructures. A user holding (2) cannot register, modify or delete any CI without approval. Any operation on a CI produces a request that must be reviewed and accepted by a user holding privilege (4). Once accepted or rejected, a notification is sent to the user.
(3) Management of CI data [Administración de datos del catálogo]	Grants the capability to access and manage the CI data and related information of the TOE, in accordance with visibility conditions and the explicitly permitted critical infrastructures.

	A user holding (3) can register, modify or delete a CI without approval.
(4) Access to new/deletion/modification CI requests [Consulta de las solicitudes de alta/baja/modificación de Infraestructuras]	Grants access to requests made by users holding (2). A user holding (4) can review the requests made, and accept or reject them. Besides, a user holding this privilege in conjunction with (2) is equivalent to (3).
(5) Administration of the audit tool [Administración de la herramienta de auditoría]	Grants access to the audit tool of the TOE.
(6) Execution of platform synchronization [Ejecución de sincronización de Plataformas]	Grants the capability to perform the synchronization of CI data (export).
(7) Management of System security attributes [Administración de atributos de seguridad del Sistema]	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)
(8) System administration [Administración de la configuración del sistema]	Grants the capability to manage the system configuration (i.e. any parameter not related to security).
(9) Access to documents [Consulta de documentos]	Grants read access to the documents managed by the Document Management Subsystem.
(10) Management of documents [Administración de documentos]	Grants full access (read / write / creation / deletion) to the documents managed by the Document Management Subsystem.

Table 1 TOE Privileges

31 Next roles are initially supported by the TOE, though new roles can be created on demand by the Security Administrator if future needs arise:

Role	Assigned privileges
ADMINISTRATOR	(1), (8)

[*ADMINISTRADOR*]	
SECURITY ADMINISTRATOR [*ADMINISTRADOR SEGURIDAD*]	(7)
OPERATOR [OPERADOR]	(1), (3), (4), (6), (9), (10)
CI OPERATOR [*OPERADOR IC*]	(1), (2), (9)
FCSE	(1), (2)
AUDITOR [AUDITOR]	(5)

Table 2 Initial Roles in the TOE

PI3 Access Control Policy (PI3AC)

32 The TOE implements an Access Control Policy named *PI3 Access Control Policy* (PI3AC Policy). This Policy is enforced by the TOE along with the RBAC Policy to assure that users have access to authorised CI Data only. It should be mentioned that this Policy is enforced when the access requested implies accessing CI Data, excepting during the synchronization. The reason lies in the necessity to the export all the information of the CI Data that needs to be synchronized. In any case, the operator will not have access to the plain text of such CI Data, since it is encrypted before leaving the TOE.

33 In particular, PI3AC Policy controls the critical infrastructures data (CI Data) a user can access to. CI Data consists of several blocks of information, each block containing several fields of data (see Table 1 Blocks of Information in HERMES). However, the need to know of each user differs. Not every user with granted access to the CI Data and enforced by RBAC Policy (users holding roles with privilege "Visualize information classified as LIMITED DISSEMINATION") should access every critical infrastructure contained in HERMES-PI3, or retrieve all data from the critical infrastructures the user has access to. Therefore, RBAC Policy is firstly enforced, and, if the user holds the appropriate privilege, then the PI3AC Policy is applied.

Eliminado: Table 1 Blocks of Information in HERMES

34 To control the access of users to the particular critical infrastructures and their information, PI3AC Policy manages visibility conditions and a explicitly permitted critical infrastructures list for each user enforcing that:

35 – The **explicitly permitted critical infrastructures** imply that each user is granted access to a specific set of critical infrastructures (CI Data).

36 – The **visibility conditions** imply that, for those critical infrastructures, the user has access only to specific fields of information to which he is authorised.

37 For example, a user may be given a restricted access to just those critical infrastructures that are managed by the enterprise he belongs to. Consequently, the user would not be granted access to information of critical infrastructures operated by a different enterprise. In a more restrictive configuration, the user may be given a restricted access to the information of a subset of those infrastructures.

38 Moreover, PI3AC Policy can limit the information of those infrastructures that is shown to the user. For instance, the user may only be able to visualize the sector and subsector that defines the infrastructure, region where the infrastructure is located, and protection measures implemented by the critical infrastructure, not being able to visualize the rest of fields.

39 RBAC and PI3AC Policies are complementary between them, since RBAC focuses on the Web resources and actions on those resources, while PI3AC focuses on the information delivered once the access to the resource is granted.

User accounts

40 User accounts are managed by the Security Administrator, or any user with a role that holds the required privilege.

41 A user account basically consists of:

- User data

42 General and contact information of the user.

- Credentials

43 The TOE supports two types of authentication methods: password-based and X.509 certificate-based.

44 The password-based authentication is always enabled for every user account, and cannot be disabled. The password is valid for a limited period of time, after which it must be changed by the legitimate user. Furthermore, the number of unsuccessful login attempts is limited and configured by the security administrator. In case the threshold is overcome, the user account is blocked. The security administrator, after analysing the related events, can decide either re-generating a new password or deleting the user account. A defined number of passwords is also remembered by the TOE for each user account. As a result, the user is forced to use a minimum number of different passwords during consecutive password renewals.

45 The security administrator can optionally enable the X.509 certificate-based authentication. The system always tries to firstly authenticate the user requesting a digital certificate. If failed or cancelled by the user, a username and password is requested. Consequently, the X.509 certificate-based method takes precedence over the password-based method during the authentication procedure.

46 The system is designed to manage a list of supported Certification Authorities (CA). When the X.509 certificate-based authentication is enabled, the security administrator must select which CAs from those supported by the system are linked to the user account. Afterwards, the user will only be able to enrol certificates issued by these CAs.

47 The auto-enrolment is the process by which a user can associate an X.509 certificate to her account, being able to authenticate using that particular certificate. There is no constraint respecting the certificates to be auto-enrolled, provided that the certificate is issued by one of the linked CAs.

- State of the user account

48 As mentioned above, the system automatically blocks a user account if the threshold of maximum login attempts is reached.

49 The security administrator can also block a user account on demand (e.g. the user account is suspected of being used maliciously). The security administrator can know, at any time, the number of login attempts for any user account.

- Roles

50 See section above “Role-Based Access Control Policy (RBAC): Roles of the TOE users and privileges”.

- Visibility conditions

51 A user can be restricted to visualize only certain fields of the blocks of information that define a critical infrastructure. This configuration is used by the TOE to enforce the PI3AC Policy.

- Explicitly permitted critical infrastructures

52 Finally, a user can be restricted to have access to a specific set of critical infrastructures (CI Data). This list is used by the TOE to enforce the PI3AC Policy.

53 The result is a complete, consistent and administrable security layer that provides robust and secure authentication and authorization of users, assuring the confidentiality of the CI Data.

Authentication procedure

54 The TOE always verifies the credentials assigned to a user before allowing her performing any action or accessing any resource, that is, before the RBAC and PI3AC Policies are enforced.

55 The user must always be authenticated before accessing the TOE and, occasionally, before performing certain sensible operations (i.e. synchronizing the CI Data, creating a user account, etc.).

56 The TOE will first try to authenticate the user using a valid X.509 certificate. The steps the TOE follows in this case are the next:

57 1. The TOE requests the user to select a digital certificate for the authentication.

58 2. The user decides to use an already enrolled certificate, and selects it. An SSL/TLS mutual authenticated channel is established between the user Web browser and the Web Application server (outside the TOE). This certificate is then retrieved by the TOE.

59 3. The TOE verifies that the certificate has been issued by a supported CA and that this CA is linked to the user account.

60 4. The TOE verifies the integrity of the certification chain, using the corresponding CA.

61 5. The TOE verifies the revocation status of the certificate using the validation service configured for the Certification Authority that issued the user's certificate. In the current version of the TOE, the supported type of validation service includes only Online Certificate Status Protocol (OCSP) services over HTTP/HTTPS. The parameters of the service (URL, port, SSL authentication, SSL certificates, etc.) are configured for each service. Each Certification Authority is configured to use one or more validation services, ordered by priority (if the first service fails to deliver the status of the certificate, the TOE invokes the second one, and so forth).

62 If the user cancels the operation in step 2, the TOE will perform the next actions:

63 1. An SSL/TLS with server authentication is established between the user Web browser and the Web Application server (outside the TOE).

64 2. The TOE will request the user to enter a username and password.

65 3. The TOE will calculate the SHA-256 hash value of the password and verify that it matches the one stored in the Data Base.

Physical boundaries

66 Next Figure 2 shows the TOE physical boundary. It is not the purpose of the figure to provide a detailed network or system architecture but to show the context where HERMES-PI3 is deployed and to identify the elements that may interact with the TOE and the physical boundaries among them.

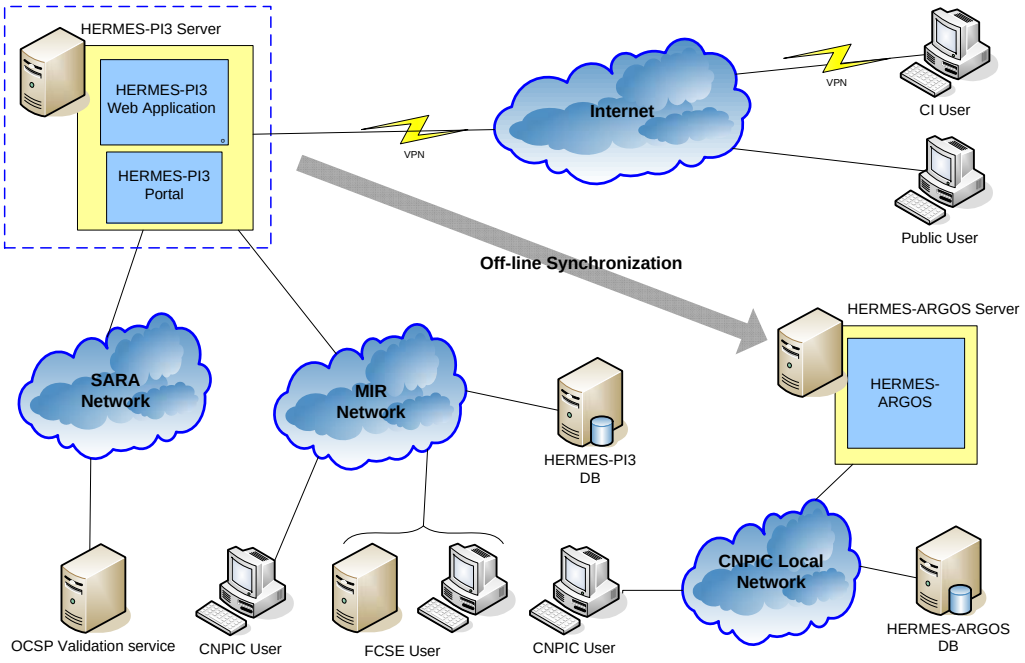


Figure 2 TOE physical boundary

67 Only one element is framed with a blue discontinuous line: HERMES- PI3 Server.

68 As can be seen 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.

69 The TOE comprises the Java classes, configuration files and associated documentation:

70 - The Java classes and configuration files are collected in a single Web Application Archive (.war).

71 – The documentation is provided to the end users and administrators separately, and includes: 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 and HERMES PI3 - Manual de Usuario.

72 As a result, the TOE does not include any hardware or firmware.

73 Users that need to have access to the services published and deployed in the HERMES-PI3 Server (the Web Application) must connect through the Local Network where the server is deployed.

Logical boundaries

74 Next Figure 3 shows the overview of TOE logical boundaries.

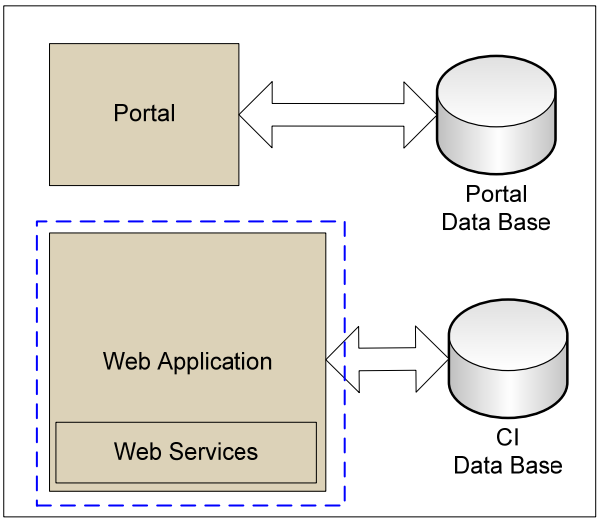


Figure 3 Overview of the TOE logical boundary

75 Figure 3 above depicts the software element that composes the **TOE**: the **Web Application**, which includes the **Web Services facade**. The Portal and Data Bases identified in the Figure, Portal Data Base and CI Data Base, are not part of the TOE, but considered part of the environment.

Web Application

76 This application offers the whole functionality for the administration and access to the CI Data by the authorised users. The application permits managing the CI Data,

performing synchronizations when needed, managing the security attributes and system parameters of the TOE, etc.

77 In any case, the operations carried out on the information belonging to the CI Data are restricted to Roles established by the Security Administrator. Furthermore, the specific information that a user can visualize depends on a set of privileges assigned by the Security Administrator to that particular user (RBAC Policy), and the visibility conditions and explicitly permitted critical infrastructures established for her user account (PI3AC).

78 HERMES-PI3 Web Application also implements a log system that records every operation performed by each user. The Web application includes an audit application to visualize the records. Thereby, the auditor of the TOE can retrieve useful information in case an unexpected event (e.g. security breach, system failure, etc.) occurs.

79 The Web Application architecture is detailed in the next Figure 4.

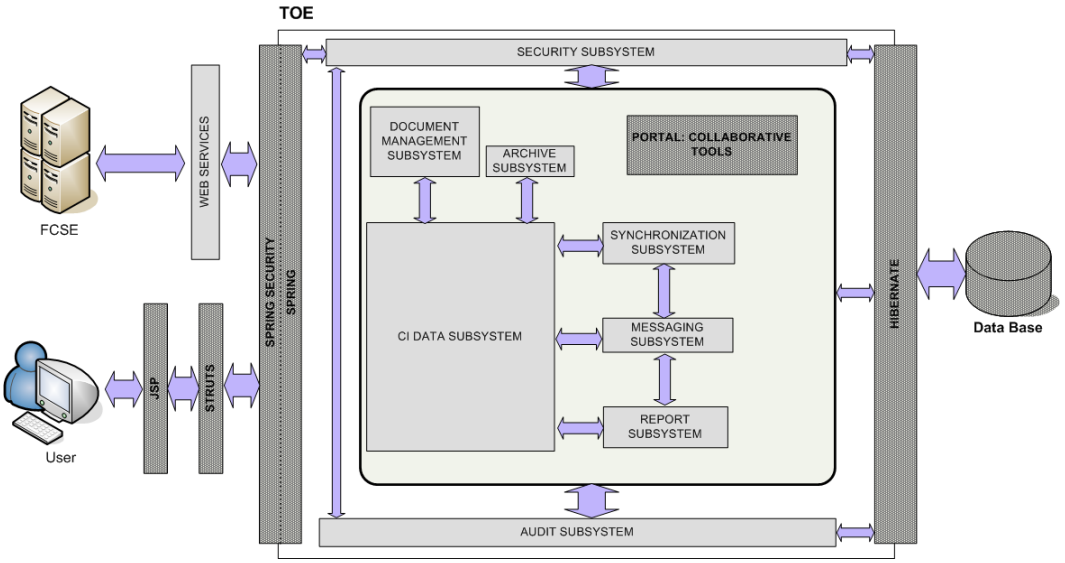


Figure 4 TOE logical boundary

80 As can be seen in Figure above, there are several subsystems inside the TOE. The elements depicted in dark grey are not part of the TOE:

Security Subsystem

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

82 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.

83 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.

84 TOE requests made through the Web Services façade are also authenticated by means of WS-Security (OASIS Web Services Security standard). Requests must be signed by the requester using a valid X.509 certificate that has to be linked to a TOE user account. The Security Subsystem takes this certificate and linked user account to authenticate the requester. Responses generated by the TOE are also signed using the functionality offered by this Subsystem. In a nutshell, SOAP messages are protected by means of WS-Security headers (XML Signatures using X.509 certificates). Thereby, peer authentication of the exchanged SOAP messages is assured. However, the mechanisms implemented by the TOE to protect the SOAP responses are out of the scope of the evaluated TOE Security Functionality (TSF).

85 Once the user is authenticated, either by the Web Service façade or the Web front-end, the requested action on the particular resource is authorised or denied by enforcing the RBAC Policy – implemented by the environment but invoked by the TOE – according to the user's role(s) and inherited privileges. In case the requested action implies accessing CI Data, the PI3AC Policy – implemented by the TOE – is also enforced according to the visibility conditions and explicitly permitted critical infrastructures assigned to the user account.

86 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

87 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

88 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

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

Archive Subsystem

90 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

91 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.

92 The cryptographic operation is carried out by the environment following the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode and with a 256-bit length key. The key is derived by the environment from a password provided by the operator, and an initialization vector (IV), salt and counter dynamically generated. The key derivation functionality complies with the Password-based Key Derivation Function 2 (PBKDF) recommended by PKCS#5 standard.

93 Both the cipher and PBKDF implementations, including the IV, salt and counter generation, are provided by the Sun Java Cryptography Extension (SunJCE), included from version 1.6 of Java Software Development Kit (Java SDK) onwards.

94 The TOE includes a wrapper of aforementioned implementations, making the details of these cryptographic operations transparent to higher layers of the application.

Messaging Subsystem

95 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

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

Web Services Subsystem

97 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.

98 Security measures for protecting SOAP messages are delegated to the Security Subsystem.

Conformance claims

CC Conformance Claim

99 This Security Target complies with the Common Criteria, version 3.1, revision 3, July 2009, for both the content and presentation requirements.

100 All functional and assurance security requirements laid out in this Security Target comply with CC Part 2 extended and CC Part 3 respectively of the above mentioned Common Criteria version.

101 Evaluation Assurance Level 2 (EAL2+), augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1.

PP Claim, Package Claim

102 This Security Target does not comply with any Protection Profile, but rather reflects the unique security properties of the TOE.

Security Problem Definition

TOE assets

103 The asset of the TOE is the CI Data, either when stored in the CI Data Base or in the portable storage device during a synchronization process.

- **A.CONF**;

104 CI Data confidentiality is ensured to be maintained through the operation of the TOE and during a synchronization process.

105 The assets herein considered include:

1. The confidentiality of the CI Data;

Threats

Expected threats to the TOE assets

106 The expected attackers are qualified so as to have a basic attack potential, in accordance with the security assurance given by AVA_VAN.2 Vulnerability analysis.

107 The expected threats may be:

108 1. Any agent external to the TOE environment, trying to gain access to the CI Data by compromising or bypassing the security measures implemented by the TOE. The attack may be performed online (through the network) or offline (manipulating the portable storage device used during the synchronization process).

109 2. An authenticated user (Administrator, Operator, Critical Infrastructure Operator, FCSE, Auditor) trying to obtain information for which she is not authorised. This threat always corresponds to an online attack and once the user has been correctly authenticated in the TOE.

110 Therefore, attacks from the inside (e.g. malware, physical access to the server, etc.) are not considered, and must be counteracted by the environment where the TOE is installed.

111 The TOE has been designed to be mitigate the next threats:

- **T.ACCESS;**

112 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;**

113 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.

114 Thus, these threats are focused on compromising the confidentiality of the CI Data.

Assumptions

Assumptions on the operational environment

- **AS.TERMINAL;**

115 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**;

116 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**;

117 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**;

118 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**;

119 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**;

120 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**;

121 It is assumed that TOE users holding the privilege (6) Execution of platform synchronization and/or (7) Management of System security attributes (see Table 1 TOE Privileges above) behave according to what it is expected, and do not act in a malicious manner.

Organizational Security Policies

- **OSP.USAGE**;

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

- **OSP.MANUAL**

123 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.

Security Objectives

Security Objectives for the TOE

- **O.MNT;**

124 The TOE shall provide an administration tool to manage the security attributes of the TOE, including: management of roles (privileges and operations associated to a role) and management of users' account (roles assignment, credentials configuration, etc.).

- **O.AUTH;**

125 The TOE shall implement an authentication mechanism to ensure the identity of the users accessing the TOE.

- **O.ACCESS**

126 The TOE shall implement an access control policy that enforces visibility conditions and an access control list based on explicitly permitted critical infrastructures for authenticated users in a manner that those users have access to the pieces of information of each CI Data to which have been authorised.

- **O.DELEGATED_ACCESS**

127 The TOE shall ensure the enforcement of the role-based access control policy implemented by the environment for each access requested by an authenticated user.

- **O.SYN;**

128 The TOE shall delegate the environment to derive the encryption key and encrypt the CI Data accordingly during the export operation of the synchronization procedure, and before the information is sent to the Applet.

- **O.AUDIT;**

129 The TOE shall implement an audit system that records every relevant security issue or event occurred during the TOE start-up, configuration, operation or shutdown. These audit records shall be accessed by authorised users only.

Security Objectives for the Operational Environment

- **OE.ACCESS;**

130 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**

131 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**

132 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;**

133 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;**

134 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;**

135 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;**

136 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;**

137 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**;

138 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;**

139 The TOE users holding privilege (6) Execution of platform synchronization and/or (7) 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 privilege (6) 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;**

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

- **OE.MANUAL**

141 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.

Security Objectives rationale

142 The following table shows the correspondence between the security objectives applicable to the TOE and the countered threats, the assumptions and the organizational security policies. Each threat, assumption and organizational security policy is addressed by one or more security objective.

	T.ACCESS	T. SYN	AS.TERMINAL	AS.PLATFORM	AS.DB	AS.PHYSICAL	AS.NETWORK	AS.GIS	AS.PERSONNEL	OSP.USAGE	OSP.MANUAL
O.MNT	X										
O.AUTH	X										
O.ACCESS	X										
O.DELEGATED_ACCESS	X										
O.SYN		X									
O.AUDIT	X	X									
OE.ACCESS	X										
OE.SYN		X									
OE.DESTRUCTION		X									
OE.TERMINAL			X								
OE.PLATFORM				X							
OE.DB					X						
OE.PHYSICAL						X					
OE.NETWORK							X				
OE. GIS								X			

	T.ACCESS	T. SYN	AS.TERMINAL	AS.PLATFORM	AS.DB	AS.PHYSICAL	AS.NETWORK	AS.GIS	AS.PERSONNEL	OSP.USAGE	OSP.MANUAL
OE.PERSONNEL		X							X		
OE.USAGE										X	
OE.MANUAL											X

Table 3 Security problem definition and security objectives

143 Next, the rationale for each matching is provided:

144 **T.ACCESS** establishes that an attacker attempts to access TOE resources for which she is not authorised by impersonating a legitimate user with such privileges. The attacker can be either an authenticated user or an external agent. This threat is counteracted by the identification, authentication and access control mechanisms and the supporting management and audit functions. In particular, **O.AUTH** implements an authentication mechanism that ensures the identity of the users accessing the TOE. On the other hand, by **O.ACCESS** the TOE implements an access control policy that enforces visibility conditions and an access control list based on explicitly permitted critical infrastructures for authenticated users in a manner that those users have access to the pieces of information of each CI Data to which have been authorised. This access control policy is complemented by the role-based access control policy implemented by the environment (**OE.ACCESS**), and invoked by the TOE (**O.DELEGATED_ACCESS**), ensuring that every authenticated user holds the adequate privileges to access the required resources. In particular, the TOE assures that the role-based access control policy is applied by delegating such enforcement to the environment for each access required by an authenticated user. In addition, the environment implements the role-based access control policy in a way that assures that users only access the authorised resources. The role-based access control policy implemented by the environment receives from the TOE the security attributes bound to user identity, such as the role(s) and privilege(s), to apply the restrictions on the user operations. Finally, **O.MNT** provides the administration tool to manage the users' accounts, including roles and authentication credentials, while **O.AUDIT** permits to detect any security breach and react accordingly.

145 **T.SYN** covers a threat where an unauthorised user attempts to gain access to the information stored in the portable storage device during a synchronization process,

or afterwards. This threat is counteracted by two Security Objectives for the TOE: **O.SYN**, which requests the TOE to delegate the environment to implement the cryptographic operations needed to encrypt the information to be synchronized; and **O.AUDIT**, which permits to detect any security breach and react accordingly. But this threat is also counteracted by three Security Objectives for the Environment: **OE.SYN**, by which the environment must implement the required cryptographic operations such as key derivation and data encryption; **OE.DESTRUCTION**, by which the environment securely destroys the portable storage device or the information therein contained in order to avoid an attacker gain access to the CI Data; and **OE.PERSONNEL**, by which TOE users holding privilege (6) Execution of platform synchronization, and/or that will manage the portable storage device used in a synchronization, prevent unauthorised entities from accessing the information contained in such device.

146 The correspondence between assumptions **AS.TERMINAL**, **AS.PLATFORM**, **AS.DB**, **AS.PHYSICAL**, **AS.NETWORK**, **AS.GIS**, **AS.PERSONNEL**, and Organizational Security Policies **OSP.USAGE** and **OSP.MANUAL** can be trivially seen in the table, meeting the corresponding Security Objectives for the Operational Environment.

Extended Components Definition

147 This section contains four extended components:

148 Two components are defined for CC Part 3 Functional Cryptographic Support Class (FCS), in particular, FCS_CKM.5 component for FCS_CKM Family, and FCS_COP.2 component for FCS_COP Family.

149 These two extended components are needed because the TOE does not implement any cryptographic operation on its own but relies on an external cryptographic provider (Sun Java Cryptography Extension Provider). However, CC Part 2 does not contain any Security Functional Requirement component that could be mapped to this requirement.

150 The other two components are defined for CC Part 3 Functional User Data Protection Class (FDP), in particular, FDP_ACC.3 component for FDP_ACC Family, and FDP_ACF.2 component for FDP_ACF Family.

151 These other two extended components are needed because though the environment is delegated to enforce the Role-Based Access Control Policy, the TOE still needs to invoke it to assure the correct access control for every user. CC Part 2 does not contain any Security Functional Requirement component that could implement this requirement.

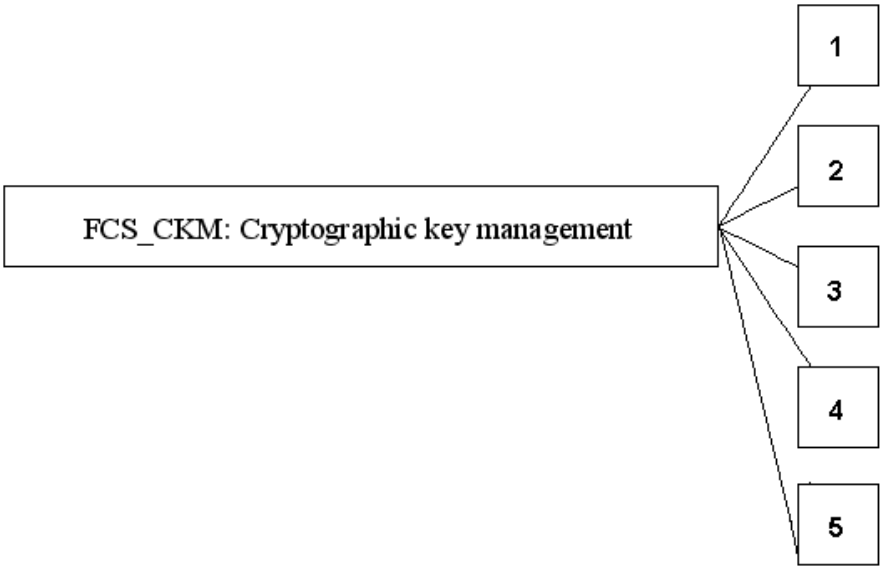
Cryptographic key management (FCS_CKM)

Family behaviour

152 Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

153 Component 5 has been added as an extended component to fulfil the aforementioned TOE requirement.

Component levelling



154 FCS_CKM.1 Cryptographic key generation, FCS_CKM.2 Cryptographic key distribution, FCS_CKM.3 Cryptographic key access and FCS_CKM.4 Cryptographic key destruction, as specified in CC Part 2.

155 FCS_CKM.5 Delegated cryptographic key derivation, requires cryptographic keys to be derived by an entity external to the TOE, in accordance with a specified key derivation function and key sizes which can be based on an assigned standard.

156 **Management: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_CKM.5**

157 There are no management activities foreseen.

158 **Audit: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_CKM.5**

159 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

160 a) Minimal: Success and failure of the activity.

161 b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.5 Delegated cryptographic key derivation

Dependencies: FCS_COP.2 Delegated cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall invoke an external entity to derive cryptographic keys in accordance with a specified cryptographic key derivation algorithm [assignment: *cryptographic key derivation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key size*] that meet the following: [assignment: *list of standards*].

Cryptographic operation (FCS_COP)

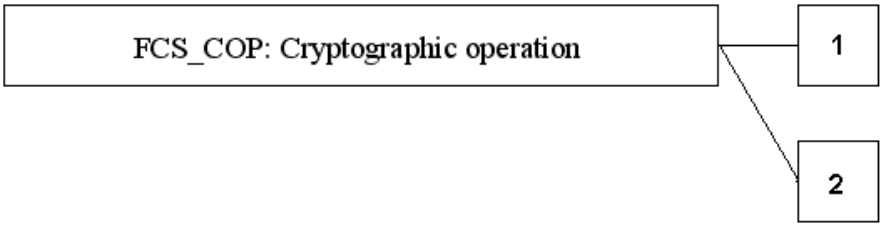
Family behaviour

162 In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

163 Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

164 Component 2 has been added as an extended component to fulfil the aforementioned TOE requirement.

Component levelling



165 FCS_COP.1 Cryptographic operation, as specified in CC Part 2.

166 FCS_COP.2 Delegated cryptographic operation, requires a cryptographic operation to be performed by an entity external to the TOE, in accordance with a specified

algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

167 **Management: FCS_COP.1, FCS_COP.2**

168 There are no management activities foreseen.

169 **Audit: FCS_COP.1, FCS_COP.2**

170 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

171 a) Minimal: Success and failure, and the type of cryptographic operation.

172 b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.2 Delegated cryptographic operation

Dependencies: FCS_CKM.5 Delegated cryptographic key derivation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 The TSF shall invoke an external entity to perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Access control policy (FDP_ACC)

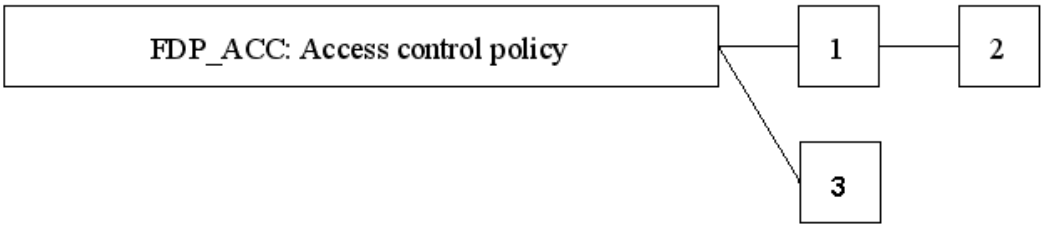
Family behaviour

173 This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allows multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named access control policy. The rules that define the functionality of an access control SFP will be defined by other families such as Access control functions (FDP_ACF) and Export from the TOE (FDP_ETC). The names of the access control SFPs identified here in Access control policy (FDP_ACC) are meant to be

used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "access control SFP."

174 Component 3 has been added as an extended component to fulfil the aforementioned TOE requirement.

Component levelling



175 FDP_ACC.1 Subset access control and FDP_ACC.2 Complete access control, as specified in CC Part 2.

176 FDP_ACC.3 Delegated complete access control, requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations protected by the TSF are covered by at least one identified access control SFP, which must be defined and implemented by an entity external to the TOE.

177 **Management: FDP_ACC.1, FDP_ACC.2, FDP_ACC.3**

178 There are no management activities foreseen.

179 **Audit: FDP_ACC.1, FDP_ACC.2, FDP_ACC.3**

180 There are no auditable events foreseen.

FDP_ACC.3 Delegated complete access control

Dependencies: FDP_ACF.2 Delegated security attribute based access control

FDP_ACC.3.1 The TSF shall invoke an external entity to enforce the [assignment: *access control SFP*] on [assignment: list *of subjects and objects*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.3.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

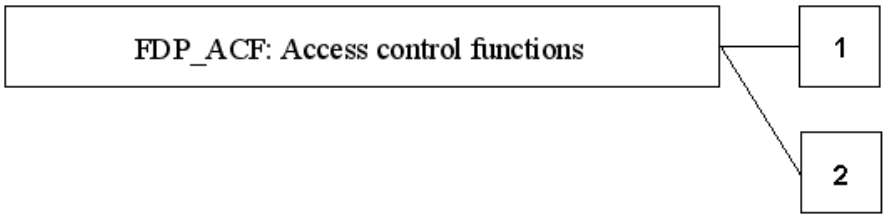
Access control functions (FDP_ACF)

Family behaviour

181 This family describes the rules for the specific functions that can implement an access control policy named in Access control policy (FDP_ACC). Access control policy (FDP_ACC) specifies the scope of control of the policy.

182 Component 2 has been added as an extended component to fulfil the aforementioned TOE requirement.

Component levelling



183 FDP_ACF.1 Security attribute based access control, as specified in CC Part 2.

184 FDP_ACF.2 Delegated security attribute based access control, allows the TSF to delegate an external entity to enforce access based upon security attributes and named groups of attributes, which may be partially specified by the TOE.

185 **Management: FDP_ACF.1, FDP_ACF.2**

186 The following actions could be considered for the management functions in FMT:

187 a) Managing the attributes used to make explicit access or denial based decisions.

188 **Audit: FDP_ACF.1, FDP_ACF.2**

189 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

190 a) Minimal: Successful requests to perform an operation on an object covered by the SFP.

191 b) Basic: All requests to perform an operation on an object covered by the SFP.

192 c) Detailed: The specific security attributes used in making an access check.

FDP_ACF.2 Delegated security attribute based access control

Dependencies: FDP_ACC.3 Delegated complete access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.2.1 The TSF shall invoke an external entity to enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.2.2 The TSF shall invoke an external entity to enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

Security Requirements for the TOE

Security Functional Requirements

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: *minimum*] level of audit; and [assignment:

- ***Start-up and shut down of the TOE.***
- ***Initialization and finalization of a session of a user.***
- ***Attempts of initiating a session.***
- ***Changes of privileges assigned to any Role.***
- ***Access to the security information of the TOE (users and roles management).***
- ***Access to classified information (CI Data)***
- ***Generation of reports containing classified information (CI Data)***
- ***Unsuccessful attempts to access the TOE resources.***

  in accordance with requirements established in CCN-STIC-301, and

- ***Synchronization processes.*****].**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *none*].

FAU_GEN.2 User identity association

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *the Auditor*] with the capability to read [assignment: *all the information generated by the audit system*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *selection and filtering*] of audit data based on [assignment: *the type of event, a*

period of time, the involved user and/or additional data to be used as a search pattern].

FCS_CKM.5 Delegated cryptographic key derivation

Dependencies: FCS_COP.2 Delegated cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall invoke an external entity to derive cryptographic keys in accordance with a specified cryptographic key derivation algorithm [assignment: *encryption key derivation following Password based Key Derivation Function 2 (PBKDF2)*] and specified cryptographic key sizes [assignment: *256 bits*] that meet the following: [assignment: *PKCS#5 v2.0 standard*].

FCS_COP.2 Delegated cryptographic operation

Dependencies: FCS_CKM.5 Delegated cryptographic key derivation

FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 The TSF shall invoke an external entity to perform [assignment: *data encryption*] in accordance with a specified cryptographic algorithm [assignment: *Advanced Encryption Standard (AES)*] and cryptographic key sizes [assignment: *256 bits*] that meet the following: [assignment: *AES in CBC mode basing on the Password based Encryption Scheme 2 (PBES2), in encryption operation, and according to PKCS#5 v2.0 standard*].

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *PI3 Access Control (PI3AC) Policy*] on [assignment:

- ***Subjects: Users of the TOE.***
- ***Objects: CI Data and fields of the CI Data.***
- ***Operations: All operations among subjects and objects that imply accessing CI Data excepting the synchronization process.*].**

FDP_ACC.3 Delegated complete access control

Dependencies: FDP_ACF.2 Delegated security attribute based access control

FDP_ACC.3.1 The TSF shall invoke an external entity to enforce the [assignment: *Role-based Access Control (RBAC) Policy*] on [assignment:

- ***Subjects: Users of the TOE.***
- ***Objects: Web resources available through the TOE, including the security attributes used by the PI3 Access Control Policy – visibility conditions and explicitly permitted critical infrastructures –, and CI Data.***

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.3.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 **The TSF shall enforce the [assignment: *PI3 Access Control (PI3AC) Policy*] to objects based on the following: [assignment:**

- ***Subjects: User identity and the associated visibility conditions and explicitly permitted critical infrastructures.***
- ***Objects: CI Data and fields of the CI Data.*].**

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *the visibility conditions and explicitly permitted critical infrastructures assigned to the user account of the authenticated user permits the access to the object*].**

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].**

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the [assignment: *none*].**

FDP_ACF.2 **Delegated security attribute based access control**

Dependencies: FDP_ACC.3 Delegated complete access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.2.1 **The TSF shall invoke an external entity to enforce the [assignment: *Role-based Access Control (RBAC) Policy*] to objects based on the following: [assignment:**

- ***Subjects: User's identity and credentials based on the assigned role(s) and inherited privileges.***
- ***Objects: Web resources available through the TOE, including the security attributes used by the PI3 Access Control Policy – visibility conditions and explicitly permitted critical infrastructures –, and CI Data.*].**

FDP_ACF.2.2 **The TSF shall invoke an external entity to enforce the following rules to determine if an operation among controlled subjects and controlled**

objects is allowed: [assignment: *the set of privileges assigned to the role(s) of the authenticated user permits the operation on the object*].

FDP_ETC.1 Export of user data without security attributes

Dependencies: FDP_ACC.1 Subset access control

FDP_ETC.1.1 The TSF shall enforce the [assignment: *Role-based Access Control (RBAC) Policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

193 **Application note 1**: The information exported from the TOE corresponds to the CI Data.

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *an administrator configurable positive integer within [assignment: 1-5]*] unsuccessful authentication attempts occur related to [assignment:

- ***Authentication of users in the TOE.***
- ***Re-authentication of users in operations that demand it.*].**

"administrator" refers to the Security administrator as defined by the TOE description.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment: *warn the user about the failure at the authentication, block the user's account and close the session, if initiated*].

FIA_ATD.1 **User attribute definition**

Dependencies: no dependencies

FIA_ATD.1.1 **The TSF shall maintain the following list of security attributes belonging to individual users: [assignment:**

- ***General information: user's name, contact telephone number and email address.***
- ***Credential information: Last date of password change, password expiration date, minimum number of different consecutive passwords (for password renewal), maximum number of unsuccessful authentication attempts, X.509 certificate-based authentication enabled/disabled, Certification Authorities assigned as valid (if X.509 certificate-based authentication is enabled).***
- ***State of the user account: Blocked/Active, Cause of blocking (if blocked), maximum number of unsuccessful authentication attempts reached.***
- ***Roles assigned, and privileges inherited from each Role.***
- ***Visibility conditions (permitted fields of CI Data).***
- ***Explicitly permitted critical infrastructures.*****].**

FIA_SOS.1 **Verification of secrets**

Dependencies: no dependencies

FIA_SOS.1.1 **The TSF shall provide a mechanism to verify that secrets meet [assignment:** ***the password quality metrics (minimum length, mandatory use of special characters and/or mandatory use of numbers) defined by the Security Administrator*****].**

FIA_SOS.2 **TSF Generation of secrets**

Dependencies: no dependencies

FIA_SOS.2.1 **The TSF shall provide a mechanism to generate secrets that meet [assignment: *the password quality metrics (minimum length, mandatory use of special characters and/or mandatory use of numbers) defined by the Security Administrator*].**

FIA_SOS.2.2 **The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *Password-based authentication mechanism*].**

FIA_UAU.2 **User authentication before any action**

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 **The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

FIA_UAU.5 **Multiple authentication mechanisms**

Dependencies: no dependencies

FIA_UAU.5.1 **The TSF shall provide [assignment:**

- ***Password-based authentication***
- ***X.509 certificate-based authentication***]

to support user authentication.

FIA_UAU.5.2 **The TSF shall authenticate any user's claimed identity according to the [assignment:**

- ***Preference of applying an X.509 certificate-based authentication mechanism first, and if cancelled by the user, a username and password-based one.***
- ***The user is able to authenticate using an X.509 certificate provided that the user account has been enabled by the Security Administrator to permit authentication by means of X.509 certificates.***].

FIA_UAU.6 **Re-authenticating**

Dependencies: no dependencies

FIA_UAU.6.1 **The TSF shall re-authenticate the user under the conditions [assignment:**

- ***Every time the Security Administrator accesses the functionality for security attributes management.***
- ***Every time a user performs a synchronization procedure.***
- ***When a user decides to change her password.***
- ***After the specified user inactivity period has elapsed.*****].**

194 **Application note 2**: The inactivity period is configured outside the TOE boundaries. In particular, the inactivity period is configured and enforced by the Web Application Server and Spring Security Framework.

FIA_UID.2 **User identification before any action**

Dependencies: no dependencies

FIA_UID.2.1 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

FIA_USB.1 **User-subject binding**

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 **The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment:**

- ***Role(s).***
- ***Inherited privilege(s).***
- ***Visibility conditions.***

- ***Explicitly permitted critical infrastructures***].

FIA_USB.1.2 **The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *none*].**

FIA_USB.1.3 **The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *none*].**

FMT_MSA.1 RBAC **Management of security attributes**

Dependencies: FDP_ACC.1 Subset access control

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **The TSF shall enforce the [assignment: *Role-based Access Control (RBAC) Policy*] to restrict the ability to [selection: *change_default, query, modify, delete*] the security attributes [assignment:**

- ***Privileges assigned to Roles.***
- ***Roles assigned to user accounts.*]**

to [assignment: *the Security Administrator*].

195 **Application note 3**: The Role-based Access Control (RBAC) Policy is defined and implemented by the environment (Spring Security Framework). The TOE assures its enforcement by invoking the environment to control any operation of any authenticated user (subject) on the objects, as defined in FDP_ACC.3 above. However, the TOE manages certain security attributes that have an impact on the behaviour of the RBAC Policy, as described in FMT_MSA.1 RBAC.

FMT_MSA.1 PI3AC **Management of security attributes**

Dependencies: FDP_ACC.1 Subset access control

FMT_SMR.1 Security Roles

FMT_MSA .1.1 The TSF shall enforce the [assignment: *PI3 Access Control (PI3AC) Policy*] to restrict the ability to [selection: *change_default, query, modify, delete*] the security attributes [assignment:

- ***Visibility conditions assigned to user accounts.***
- ***Explicitly permitted critical infrastructures assigned to user accounts.*]**

to [assignment: *the Security Administrator*].

196 **Application note 4**: The PI3 Access Control (PI3AC) Policy is defined and implemented by the TOE. The TOE manages certain security attributes that have an impact on the behaviour of the PI3AC Policy, as described in FMT_MSA.1 PI3AC. However, it should be noted that the access control policy enforced to change_default, query, modify or delete these attributes is the RBAC Policy, by which the capability to perform these operations is limited to the Security Administrator.

FMT_MSA.3 RBAC Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Role-based Access Control (RBAC) Policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *Security Administrator*] to specify alternative initial values to override the default values when an object or information is created.

197 **Application note 5**: The Role-based Access Control (RBAC) Policy is defined and implemented by the environment (Spring Security Framework). The TOE assures its enforcement by invoking the environment to control any operation of any authenticated user (subject) on the objects, as defined in FDP_ACC.3 above. However, the TOE initializes certain security attributes with default values and that have an impact on the behaviour of the RBAC Policy, as described in FMT_MSA.3 RBAC. In particular, the roles are initially instantiated with no privileges assigned

and no role assigned, although the Security Administrator can modify these parameters before a user account object is created in the TOE.

FMT_MSA.3 PI3AC Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *PI3 Access Control (PI3AC) Policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *Security Administrator*] to specify alternative initial values to override the default values when an object or information is created.

198 **Application note 6**: The PI3 Access Control (PI3AC) Policy is defined and implemented by the TOE. The TOE enforces it to control the access to CI Data by any authenticated user (subject), as defined in FDP_ACC.1 above. However, the TOE initializes certain security attributes with default values and that have an impact on the behaviour of the PI3AC Policy, as described in FMT_MSA.3 PI3AC. In particular, users' accounts are created with null visibility conditions and no critical infrastructure explicitly permitted, although the Security Administrator can modify these parameters before a user account object is created in the TOE.

FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*] the [assignment:

- ***On the users' information, as specified in FIA_ATD.1 User attribute definition, the operations change_default, query, modify, delete and clear.***

- ***On the roles' information, the operations change_default, query, modify, delete and clear.***
- ***On the System configuration (password quality metrics): Minimum password length, mandatory use of numbers in passwords, mandatory use of special characters in passwords, the operations change_default, query, modify, and clear.***
- ***On the System configuration (management metrics): minimum validity period (days), maximum validity period (days), minimum number of different consecutive passwords (for password renewal), maximum number of unsuccessful authentication attempts, the operation query.***
- ***On the System configuration (Web Services management): certificate used by the TOE to sign the SOAP responses, users authorised to invoke the web services published by the TOE, the operations change_default, query, modify, and clear.*]**

to [assignment: *the Security Administrator*].

FMT_MTD.2 Management of limits on TSF data

Dependencies: FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security Roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment:

- ***Validity period (days).***
- ***Minimum number of different consecutive passwords (for password renewal).***
- ***Maximum number of unsuccessful authentication attempts for user accounts.*]**

to [assignment: *the Security Administrator*].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment:

- ***When the validity period is reached, the user is obliged to change the password.***
- ***When the minimum number of different consecutive passwords is reached, the user is allowed to reuse a previous password.***

- ***When the maximum number of unsuccessful authentication attempts is reached, the user account is blocked.*****].**

FMT_REV.1 Revocation

Dependencies: FMT_SMR.1 Security Roles

FMT_REV.1.1 The TSF shall restrict the ability to revoke [assignment: *Passwords*] associated with the [selection: *users*] under the control of the TSF to [assignment: *the Security Administrator*].

FMT_REV.1.2 The TSF shall enforce the rules [assignment: *revocation will take place on the next attempt to access the TOE*].

FMT_SAE.1 Time-limited authorisation

Dependencies: FMT_SMR.1 Security Roles

FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: *Passwords*] to [assignment: *the Security Administrator*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *Force the user to renew the password*] after the expiration time for the indicated security attribute has passed.

FMT_SMF.1 Specification of Management Functions

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- ***Management of roles, including Administrator, Security Administrator, Operator, Critical Infrastructure Operator, FCSE and Auditor, by a Security Administrator.***
- ***Management of user account's general information: user's name, contact telephone number and email address, by a Security Administrator.***
- ***Management of user account's credential information: validity period, minimum number of different consecutive passwords (for password renewal), maximum number of unsuccessful authentication attempts, enabling/disabling X.509 certificate-based authentication, assign Certification Authorities as valid (if X.509 certificate-based authentication is enabled), re-generate the user's password, by a Security Administrator.***
- ***Management of state of user's account: block/activate the user account, by a Security Administrator.***
- ***Management of visibility conditions for each user account, by a Security Administrator.***
- ***Management of a list of explicitly permitted critical infrastructures for each user account, by a Security Administrator.***
- ***Management of supported Certification Authorities and validation services, by a Security Administrator.***
- ***Management of user's credentials, including: auto-enrol new X.509 certificates, and change password, by the corresponding user.***
- ***Management of the System configuration (password quality metrics): Minimum password length, mandatory use of numbers in passwords, mandatory use of special characters in passwords, by a Security Administrator.***
- ***Management of the System configuration (Web Services management): certificate used by the TOE to sign the SOAP responses, users authorised to invoke the web services published by the TOE, by a Security Administrator.*****]**

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *Administrator, Security Administrator, Operator, Critical Infrastructure Operator, FCSE and Auditor*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

199 **Application note 7**: The TOE delegates the authorisation of authenticated users basing on the Role-Based Access Control (RBAC) Policy to the environment (Spring Security Framework). The TOE implements functions to manage the roles of the TOE and bind users to roles.

Security Assurance Requirements

200 The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

201 EAL2+ ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1.

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation of evidence elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation of evidence elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation of evidence elements:

ADV_TDS.3.1C **The design shall describe the structure of the TOE in terms of subsystems.**

ADV_TDS.3.2C **The design shall describe the TSF in terms of modules.**

ADV_TDS.3.3C **The design shall identify all subsystems of the TSF.**

ADV_TDS.3.4C **The design shall provide a description of each subsystem of the TSF.**

ADV_TDS.3.5C **The design shall provide a description of the interactions among all subsystems of the TSF.**

ADV_TDS.3.6C **The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.**

ADV_TDS.3.7C **The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.**

ADV_TDS.3.8C **The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.**

ADV_TDS.3.9C **The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.**

ADV_TDS.3.10C **The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.**

ADV_IMP.1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation of evidence elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C **The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**

AGD_OPE.1.3C **The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**

AGD_OPE.1.4C **The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

AGD_OPE.1.5C **The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**

AGD_OPE.1.6C **The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.**

AGD_OPE.1.7C **The operational user guidance shall be clear and reasonable.**

AGD_PRE.1 **Preparative procedures**

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D **The developer shall provide the TOE including its preparative procedures.**

Content and presentation of evidence elements:

AGD_PRE.1.1C **The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**

AGD_PRE.1.2C **The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D **The developer shall provide the TOE and a reference for the TOE.**

ALC_CMC.2.2D **The developer shall provide the CM documentation.**

ALC_CMC.2.3D **The developer shall use a CM system.**

Content and presentation of evidence elements:

ALC_CMC.2.1C **The TOE shall be labelled with its unique reference.**

ALC_CMC.2.2C **The CM documentation shall describe the method used to uniquely identify the configuration items.**

ALC_CMC.2.3C **The CM system shall uniquely identify all configuration items.**

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D **The developer shall provide a configuration list for the TOE.**

Content and presentation of evidence elements:

ALC_CMS.2.1C **The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.**

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation of evidence elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation of evidence elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.2 Derived security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation of evidence elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C **The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**

ASE_CCL.1.10C **The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

ASE_SPD.1 **Security problem definition**

Dependencies: No dependencies.

Developer action elements:

ASE_APD.1.1D **The developer shall provide a security problem definition.**

Content and presentation of evidence elements:

ASE_SPD.1.1C **The security problem definition shall describe the threats.**

ASE_SPD.1.2C **All threats shall be described in terms of a threat agent, an asset, and an adverse action.**

ASE_SPD.1.3C **The security problem definition shall describe the OSPs.**

ASE_SPD.1.4C **The security problem definition shall describe the assumptions about the operational environment of the TOE.**

ASE_OBJ.2 **Security objectives**

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D **The developer shall provide a statement of security objectives.**

ASE_OBJ.2.2D **The developer shall provide a security objectives rationale.**

Content and presentation of evidence elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation of evidence elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation of evidence elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C **All operations shall be performed correctly.**

ASE_REQ.2.5C **Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.**

ASE_REQ.2.6C **The security requirements rationale shall trace each SFR back to the security objectives for the TOE.**

ASE_REQ.2.7C **The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.**

ASE_REQ.2.8C **The security requirements rationale shall explain why the SARs were chosen.**

ASE_REQ.2.9C **The statement of security requirements shall be internally consistent.**

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.2 Derived security requirements

ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ASE_TSS.1.1D **The developer shall provide a TOE summary specification.**

Content and presentation of evidence elements:

ASE_TSS.1.1C **The TOE summary specification shall describe how the TOE meets each SFR.**

ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D **The developer shall provide evidence of the test coverage.**

Content and presentation of evidence elements:

ATE_COV.1.1C **The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**

ATE_FUN.1 **Functional testing**

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D **The developer shall test the TSF and document the results.**

ATE_FUN.1.2D **The developer shall provide test documentation.**

Content and presentation of evidence elements:

ATE_FUN.1.1C **The test documentation shall consist of test plans, expected test results and actual test results.**

ATE_FUN.1.2C **The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.**

ATE_FUN.1.3C **The expected test results shall show the anticipated outputs from a successful execution of the tests.**

ATE_FUN.1.4C **The actual test results shall be consistent with the expected test results.**

ATE_IND.2 **Independent testing - sample**

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D **The developer shall provide the TOE for testing.**

Content and presentation of evidence elements:

ATE_IND.2.1C **The TOE shall be suitable for testing.**

ATE_IND.2.2C **The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.**

AVA_VAN.2 **Vulnerability analysis**

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D **The developer shall provide the TOE for testing.**

Content and presentation of evidence elements:

AVA_VAN.2.1C **The TOE shall be suitable for testing.**

Rationale for the Security Requirements

202 The following table shows the correspondence between the security objectives applicable to the TOE and the defined security functional requirements.

	O.MNT	O.AUTH	O.ACCESS	O.DELEGATED_ACCESS	O.SYN	O.AUDIT
FAU_GEN.1 Audit data generation						X
FAU_GEN.2 User identity association						X
FAU_SAR.1 Audit review	X					X
FAU_SAR.2 Restricted audit review	X					X
FAU_SAR.3 Selectable audit review	X					X
FCS_CKM.5 Delegated cryptographic key derivation					X	
FCS_COP.2 Delegated cryptographic operation					X	
FDP_ACC.1 Subset access control			X			

	O.MNT	O.AUTH	O.ACCESS	O.DELEGATED_ACCESS	O.SYN	O.AUDIT
FDP_ACC.3 Delegated complete access control				X		
FDP_ACF.1 Security attribute based access control			X			
FDP_ACF.2 Delegated security attribute based access control				X		
FDP_ETC.1 Export of user data without security attributes					X	
FIA_AFL.1 Authentication failure handling		X				
FIA_ATD.1 User attribute definition	X	X				
FIA_SOS.1 Verification of secrets		X				
FIA_SOS.2 TSF Generation of secrets		X				
FIA_UAU.2 User authentication before any action		X				
FIA_UAU.5 Multiple authentication mechanisms		X				

	O.MNT	O.AUTH	O.ACCESS	O.DELEGATED_ACCESS	O.SYN	O.AUDIT
FIA_UAU.6 Re-authenticating		X				
FIA_UID.2 User identification before any action		X	X	X		
FIA_USB.1 User-subject binding			X	X		
FMT_MSA.1 RBAC Management of security attributes				X		
FMT_MSA.1 PI3AC Management of security attributes			X			
FMT_MSA.3 RBAC Static attribute initialisation				X		
FMT_MSAC.3 PI3AC Static attribute initialisation			X			
FMT_MTD.1 Management of TSF data	X	X				
FMT_MTD.2 Management of limits on TSF data	X	X				
FMT_REV.1 Revocation	X	X				

	O.MNT	O.AUTH	O.ACCESS	O.DELEGATED_ACCESS	O.SYN	O.AUDIT
FMT_SAE.1 Time-limited authorisation	X	X				
FMT_SMF.1 Specification of Management Functions	X	X				
FMT_SMR.1 Security roles	X			X		

Table 4 Security objectives and functional requirements

203 **Fulfilment of Security Objective O.MNT**

204 **O.MNT** states that the TOE shall provide an administration tool to manage the security attributes of the TOE, including: management of roles and management of users' account. This objective is fulfilled by a series of SFRs:

205 1) SFRs related to audit trails management: **FAU_SAR.1 Audit review**, **FAU_SAR.2 Restricted audit review and FAU_SAR.3 Selectable audit review**. These SFRs permit to manage and access in a selectable and restricted manner the audit trails generated during the TOE start-up, shutdown, and several events related to the TOE usage and the synchronization procedure. Each logged event contains detailed information that permits the further analysis of the audit trails, like the date and time, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

206 2) **FIA_ATD.1 User attribute definition**, by which the TOE maintains a complete list of security attributes belonging to individual users, what allows the coherent management of the user accounts. This includes general information about the user, information related to the user's credential, state of the user account, roles assigned, visibility conditions and a list of explicitly permitted critical infrastructures.

207 3) SFRs related to management functions: **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** and **FMT_SMR.1 Security roles**. These SFRs provide a comprehensive and secure management of the security attributes and TSFs of the TOE.

208 The TOE management capability is enforced in a secure manner by **FMT_MTD.1 Management of TSF data** and **FMT_MTD.2 Management of limits on TSF data.**

209 **FMT_REV.1 Revocation** permits to revoke passwords in a restrictive fashion (only available for the Security Administrator), while **FMT_SAE.1 Time-limited authorisation** focuses on restricting the capability to specify an expiration time for the passwords to the Security Administrator.

210 The management functions that are available in the TOE are specified in **FMT_SMF.1 Specification of Management Functions**.

211 The initially configured roles available in the TOE and used by the TSF are described in **FMT_SMR.1 Security roles**.

212 **Fulfilment of Security Objective O.AUTH**

213 **O.AUTH** states that the TOE shall implement an authentication mechanism to ensure the identity of the users accessing the TOE. This objective is fulfilled by a wide range of SFRs.

214 The TOE performs the authentication as a former step before the access control policies are enforced. Next SFRs are focused on the TOE authentication.

215 1) SFRs **FIA_UID.2 User identification before any action** and **FIA_UAU.2 User authentication before any action** support the authentication on the users of the TOE every time an access to a resource or an action on a resource is requested, basing on the security attributes defined for the user's identity, and before allowing any other TSF-mediated actions on behalf of that user. The information for each individual user corresponds to that defined in **FIA_ATD.1 User attribute definition**, what includes general information about the user, information related to the user's credential, state of the user account, roles assigned, visibility conditions and a list of explicitly permitted critical infrastructures.

216 By means of **FIA_UAU.6 Re-authenticating**, the TOE forces the Security Administrator to re-authenticate when accessing the functionality for security attributes management. Operators that perform a synchronization procedure must also be re-authenticated, according to this SFR. In general, every user must be re-authenticated when the specified user inactivity period has elapsed.

217 **FIA_UAU.5 Multiple authentication mechanisms** extends the password-based authentication mechanism to an optional X.509 certificate-based one, enriching the methods a user can use during the identification phase.

218 The quality of the passwords used for the authentication is controlled by **FIA_SOS.1 Verification of secrets**. Initial passwords are created by the TOE and following the password quality metrics, in accordance with **FIA_SOS.2 TSF Generation of secrets**.

219 The maximum number of unsuccessful authentication attempts is restricted by **FIA_AFL.1 Authentication failure handling**. When the maximum number of attempts is reached, the user account is blocked, reducing the risk of an attacker to successfully perform a brute force attack. This policy is applied both in normal authentication processes and when a re-authentication is needed. On the other hand, thanks to **FMT_REV.1 Revocation**, users' credentials, and more specifically the user's password, can be revoked when needed by the Security Administrator, avoiding the corresponding user to enter the TOE. Finally, **FMT_SAE.1 Time-limited authorisation** permits the Security Administrator to establish an expiration time for the users' passwords. In case the expiration time has passed, this SFR forces the user to renew the password. This holistic approach achieves that only valid users with valid and active credentials are able to access the TOE.

220 2) Another set of SFRs focused on management procedures permits to enforce the authentication of TOE users by implementing the behaviour and procedures

mentioned above. These SFRs include: **FMT_MTD.1 Management of TSF data**, that restricts the ability to manage the security attributes of the TOE to the Security Administrator; **FMT_MTD.2 Management of limits on TSF data** achieve the same as the previous ones but concerning the default values assigned to the security attributes managed at System configuration level;; Finally, SFRs **FMT_SMF.1 Specification of Management Functions** specify the management functions existent. These management functions permit the definition and enforcement of the authentication mechanisms applicable inside the TOE boundaries.

221 **Fulfilment of Security Objective O.ACCESS**

222 **O.ACCESS** sets that the TOE shall implement an access control policy that enforces visibility conditions and an access control list based on explicitly permitted critical infrastructures for authenticated users in a manner that those users have access to the pieces of information of each CI Data to which have been authorised.

223 The access control policy implemented by the TOE is named PI3 Access Control (PI3AC) Policy. This policy is mainly enforced by two SFR. **FDP_ACC.1 Subset access control** specifies that the TOE shall enforce the PI3 Access Control (PI3AC) Policy on the subjects: users of the TOE; and objects: CI Data and fields of the CI Data; for every operation among subjects and objects that implies accessing CI Data excepting the synchronization process. On the other hand, **FDP_ACF.1 Security attribute based access control** particularizes the application of PI3AC basing on the visibility conditions and explicitly permitted critical infrastructures assigned to the user account of the authenticated user. The exception introduced does not violate the security objective, since the operator is not able to access the plain text of the CI Data being synchronized as it is maintained encrypted during the whole process.

224 The TOE manages certain security attributes that have an impact on the PI3AC Policy, such as the visibility conditions and explicitly permitted critical infrastructures assigned to the users' accounts. SFR **FMT_MSA.1 PI3AC Management of security attributes** and **FMT_MSA.3 PI3AC Static attribute initialisation** permit such management.

225 **FIA_UID.2 User identification before any action** permits the TOE to obtain the user identity used for the access control, while **FIA_USB.1 User-subject binding** permits the association of the security attributes visibility conditions and explicitly permitted critical infrastructures with the subject acting on the behalf of that user.

226 **Fulfilment of Security Objective O.DELEGATED_ACCESS**

227 **O.DELEGATED_ACCESS** establishes that the TOE shall ensure the enforcement of the role-based access control policy implemented by the environment for each access requested by an authenticated user.

228 SFRs **FDP_ACC.3 Delegated complete access control** and **FDP_ACF.2 Delegated security attribute based access control**, which are based on the corresponding extended components, requires the TOE to delegate the environment to define and enforce the role-based access control policy (RBAC Policy). Thereby, it is ensured that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP implemented by the environment. Furthermore, the TOE manages certain security attributes that have an impact on the RBAC Policy, such as the user's role(s) and privilege(s) assigned to the role(s). SFR **FMT_MSA.1 RBAC Management of security attributes**, **FMT_MSA.3 RBAC Static attribute initialisation** and **FMT_SMR.1 Security roles** permit such management.

229 **FIA_UID.2 User identification before any action** permits the TOE to obtain the user identity used for the access control, while **FIA_USB.1 User-subject binding** permits the association of the security attributes role(s) and inherited privilege(s) with the subject acting on the behalf of that user.

230 **Fulfilment of Security Objective O.SYN**

231 **O.SYN** sets that the TOE shall delegate the environment to derive the encryption key and encrypt the CI Data accordingly during the export operation of the synchronization procedure, and before the information is sent to the Applet. This security objective is met by four SFRs working in conjunction:

232 In order perform a correct synchronization the information must be encrypted. For that purpose, the TOE delegates the encryption operation to the environment, which uses an AES implementation in CBC mode where the encryption key is derived using a Password based Key Derivation Function 2 (PBKDF2) as defined in PKCS#5 v2.0 standard. The TOE sends the initialization vector (IV), salt and counter (dynamically generated) along with the password provided by the Operator to the Applet in order to allow the later import operation into HERMES-PI3 Platform.

233 **FCS_CKM.5 Delegated cryptographic key derivation** requires the TOE to delegate the environment to generate 256-bit length cryptographic keys in accordance with the Password based Key Derivation Function 2 (PBKDF2) defined in PKCS#5 v2.0 standard. The password must be provided by the operator before exporting the CI Data.

234 **FCS_COP.2 Delegated cryptographic operation** requires the TOE to delegate the environment to encrypt the information before exporting it out of the TOE during the synchronization by using the aforementioned dynamically generated key. Particularly, this SFR meets the requirements established in the Advanced Encryption Standard (AES), using a 256-bit length cryptographic key size in AES-CBC mode, basing on the Password based Encryption Scheme 2 (PBES2), in encryption operation, and according to PKCS#5 v2.0 standard.

235 Therefore, these two SFRs allow the TOE to encrypt the CI data to be synchronized by means of the environment and using strong cryptography and without having to deal with cryptographic material management, as requested by O.SYN security objective.

236 Finally, **FDP_ETC.1 Export of user data without security attributes** permits to export the user data (CI Data) without security attributes from the TOE, supporting the synchronization procedure.

237 **Fulfilment of Security Objective O.AUDIT**

238 **O.AUDIT** establishes that the TOE shall implement an audit system that records every relevant security issue or event occurred during the TOE start-up, configuration, operation or shutdown. Moreover, it indicates that these audit records shall be accessed by authorised users only.

239 This objective is clearly met by the SFRs specifically focused on secure audit trail generation and management: **FAU_GEN.1 Audit data generation**, **FAU_GEN.2 User identity association**, **FAU_SAR.1 Audit review**, **FAU_SAR.2 Restricted audit review** and **FAU_SAR.3 Selectable audit review**.

240 More specifically, **FAU_GEN.1 Audit data generation**, **FAU_GEN.2 User identity association** aim at generating audit trails with consistent and complete information, while **FAU_SAR.1 Audit review**, **FAU_SAR.2 Restricted audit review** and **FAU_SAR.3 Selectable audit review**'s purpose is to permit an Auditor accessing the generated logs.

241 **Justification for non-satisfied dependences**

242 SFRs FAU_GEN.1 Audit data generation and FMT_SAE.1 Time-limited authorisation depend on **FPT_STM.1 Reliable time stamps**, which is not included in the list of SFRs implemented by the TOE.

243 In the former, the audit trails incorporate the date given by the internal clock of the server where the TOE operates, not the date included in a timestamp that may be provided by a Time-stamping Authority. These trails are used by the auditor to establish evidence about the occurrence or not of a particular event or action. However, the TOE does not provide no-repudiation of evidence since non-repudiation it is not a requirement for the TOE. Therefore, the relative date provided by the TOE's server suffices for auditing purposes, providing that the clock of the server is accurately configured (see assumption AS.PLATFORM).

244 In the latter, the reliable time-stamp should be used to evaluate whether a password has expired or not, basing on the date therein contained. However, the validity period for a password is normally between 60 and 90 days. Therefore, a minimal inaccuracy in the clock of the server does not imply an impact on the actual validity of the passwords managed in the TOE.

245 SFRs **FCS_CKM.5 Delegated cryptographic key derivation** and **FCS_COP.2 Delegated cryptographic operation** depend on SFR FCS_CKM.4 Cryptographic key destruction, which is not included. Due to the programming language used to implement the TOE (Java language), and the particular Java Classes used to implement the cryptographic operations, the key destruction and zeroization depend on the Java Virtual Machine and Garbagge Collector, and thus a secure destruction at an accurate time (i.e. after synchronizing) cannot be assured.

246 Finally, FDP_ETC.1 Export of user data without security attributes and FMT_MSA.1 RBAC Management of security attributes depend on **FDP_ACC.1 Subset access control**. Instead, FDP_ACC.3 Delegated complete access control is included as an extended SFR.

247 **Rationale for the selection of the Security Assurance Requirements EAL2+ ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1**

248 The Security Assurance Requirements (SAR) have been selected according to the Evaluation Assurance Level 2+ (EAL2 augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 and ALC_TAT.1).

249 EAL2 augmented with these SFRs has been selected taking into account the security requirements established for ITC systems that manages CLASSIFIED information as specified by the *Centro Criptológico Nacional (CCN)*.

TOE Summary Specification

TOE Security Functions

250 Each security function description contains the security requirements to which it corresponds, explaining how it specifically satisfies each of its related requirements.

Identification and Authentication

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

251 A resilient identification and authentication procedure is implemented by the TOE, ensuring the identity of users accessing the TOE. The identification and authentication procedures are the first steps before the access control policies RBAC and PI3AC are enforced.

252 The available authentication mechanisms include username and password (always enabled) and X.509 certificate (optional). Each time the user tries to access the TOE she must provide the correct credentials. The TOE will firstly try to authenticate the user by means of a valid X.509 certificate. Otherwise, a username and password are requested. Moreover, the TOE requests the user to re-authenticate in certain sensitive operations, increasing the overall security. These operations include:

253 – Every time the Security Administrator accesses the functionality for security attributes management.

254 – Every time an operator performs a synchronization procedure.

255 – When a user decides to change her password.

256 – After the user inactivity period has elapsed.

257 In case of password-based authentication, the TOE initially generates a password that has to be sent to the user by using suitable means (e.g. a secure out-of-band mechanism). Afterwards, and after the user is authenticated the first time, the TOE obliges her to select a new password. The password has a defined validity period, after which the user must select a new password. The system also remembers a limited number of consecutive passwords, avoiding the user to repeat a password within that number of renewals. The TOE also allows the Security Administrator to

reset the password in case of compromise or forgetfulness. As a result, this method implicitly revokes the previous password.

258 Every time a new password is generated or selected, the TOE verifies that it meets the requirements configured in the password quality metrics. The metrics include the minimum password length, the mandatory use of special characters and/or the mandatory use of numbers. Password quality metrics can be configured by the Security Administrator, establishing the length and the use or not of special characters and/or numbers.

259 The X.509 certificate-based method verifies that the certificate received once the mutually authenticated SSL/TLS channel has been established is issued by an authorised Certificate Authority, the certificate's integrity is maintained, the certificate is within its validity period and it has not been revoked. This last operation is carried out using the validation services (OCSP) associated to the Certification Authority that issued the user's certificate.

260 When the maximum number of unsuccessful authentication attempts is reached, the TOE will block the user account. It can only be re-activated by the Security Administrator.

Access Control

FDP_ACC.1 Subset access control, FDP_ACC.3 Delegated complete access control, FDP_ACF.1 Security attribute based access control, FDP_ACF.2 Delegated security attribute based access control, FIA_USB.1 User-subject binding, FMT_MSA.1 RBAC Management of security attributes, FMT_MSA.3 RBAC Static attribute initialisation, FMT_MSA.1 PI3AC Management of security attributes and FMT_MSA.3 PI3AC Static attribute initialisation

261 The TOE implements the PI3 Access Control Policy (PI3AC Policy), by which the TOE verifies the visibility conditions and critical infrastructures a user has access to on each operation that implies accessing CI Data.

262 For that purpose, users' accounts are given with visibility conditions and a list of explicitly permitted critical infrastructures that permit the enforcement of such policy. Once the user is correctly authenticated, the TOE will associate these values with the subject identity, being able to enforce the policy from that moment onwards.

263 As an exception. PI3AC Policy is not applied during the synchronization process, as the Operator must be able to export all the information concerning the new and updated CI Data, no matter the security attributes defined for that user respecting the PI3AC Policy. In any case, the information is encrypted before leaving the TOE (see Secure Synchronization section below).

264 On the other side, the TOE delegates the definition and enforcement of the role-based access control policy to the environment. In particular, the environment implements a Role-based Access Control Policy (RBAC Policy), by which accesses to the TOE resources are authorised according to the privileges held by the authenticated user. In the same way as with PI3AC Policy, once the user is correctly authenticated, the TOE will associate the role(s) and privileges inherited by the user with the subject identity to allow the policy enforcement.

265 RBAC Policy is always enforced when a user requests access to a TOE resource. However, PI3AC Policy is only enforced when this resource corresponds to CI Data (except for the synchronization process, as commented above). Therefore, in this case, both access control policies will be enforced. The RBAC Policy will be enforced in the first place in order to decide whether the user can access CI Data or not, and PI3AC Policy afterwards, to decide what information of CI Data the user can access to.

266 The TOE manages the security attributes that are required for the enforcement of the access control policies herein described (see Management section below).

Audit System

FAU_GEN.1 Audit data generation, FAU_GEN.2 User identity association, FAU_SAR.1 Audit review, FAU_SAR.2 Restricted audit review and FAU_SAR.3 Selectable audit review

267 The TOE implements a complete log and audit system. Every action specified in FAU_GEN.1 Audit data generation, and every auditable event implicitly derived from the audit level established (minimum), is recorded in the external data base (belongs to the operational environment).

268 The TOE also provides a graphical tool that permits the auditor to retrieve in a selective fashion the audit trails, using several filtering criteria. Thereby, the auditor is capable of tracing any action or event, being able to identify the date and identity of the subject that performed the action or caused the event.

Secure Synchronization

FCS_CKM.5 Delegated cryptographic key derivation and FCS_COP.2 Delegated cryptographic operation and FDP_ETC.1 Export of user data without security attributes

269 The TOE implements a functionality to allow the operators to export information of CI Data that has been updated or created in the TOE in order to further import it into HERMES-ARGOS Platform (environment). The Operator carrying out the export operation must be authorised by means of the RBAC Policy.

270 The information is initially exported from the TOE and stored in a portable storage device. Later, the operator imports the data into HERMES-ARGOS Platform using the portable storage device and the Web interface available in the Platform.

271 The information to be stored in the device is encrypted before leaving the TOE by using a strong symmetric cryptographic algorithm (AES in CBC mode, and using a 256-bit length keys), assuring its confidentiality. The information is then sent encrypted to the Applet, which will later store it in the portable storage device. The TOE internally delegates the environment to encrypt the information before sending it to the Applet. The encryption key is derived by the environment from a password that must be provided by the operator.

272 As already mentioned the Applet (out of the scope of the TOE) is downloaded into the operator's computer and used both during the export and import operations. In particular:

273 – During the export phase, the Applet requests the operator to enter the password for the synchronization process. This password will be used by the TOE environment to derive the encryption key, as mentioned above. The Applet communicates with the TOE to send the synchronization password. Once the TOE environment has encrypted the information to be synchronized, the Applet downloads the encrypted files through the TOE interface and asks the operator to select the CD drive to use for the data storage. Additional information like the initialization vector, salt and counter (generated by the TOE environment during the initialization of the encryption scheme) and needed for the import phase is also stored in the portable device.

274 – During the import phase, the Applet asks the operator to enter the password (which must be the same as the one used in the export phase), and sends it to HERMES-ARGOS Platform along with the initialization vector, the salt and the counter. This information will permit the Platform to derive the decryption key and use the correct decryption scheme. Afterwards, the Applet uploads each file to the Platform, which delegates its decryption to the environment. Once decrypted, the Platform consolidates the required changes in the external database. It should be mentioned that if the password provided by the operator in the import phase is not the correct one, and due to the scheme used during the cryptographic operations, the Platform will detect it and will abort the process.

275 As the encryption and decryption keys are dynamically generated, any cryptographic material management is avoided. The TOE security policy establishes that this password must be kept secret during the whole process and until the portable storage device is securely destroyed or its information securely erased. Due to the cryptographic algorithms used, a different symmetric key is generated in each synchronization process, mitigating the risk of key compromise.

276 Finally, the mandatory use of a Read-Only portable storage device (e.g. CD-R) assures that modifications on the encrypted information stored in the device are not possible.

Management

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

277 The TOE implements a full set of management functions available to the administrators of the TOE through the Web Application interface. The Security Administrator is the only one who is able to configure and maintain the security attributes, including the users' accounts and roles. The Administrator can manage and administer the rest of the information related to the TOE operation. The Auditor is the only one that can access the audit system records.

278 The security-related management functions are the next:

279 a) *Management of roles, including Administrator, Security Administrator, Operator, Critical Infrastructure Operator, FCSE and Auditor.*

280 The Security Administrator can create, modify or delete roles of the TOE. A role must be assigned one or more privileges, which cannot be modified throughout the TOE operation.

281 b) *Management of user accounts,' general information: user's name, contact telephone number and email address.*

282 The Security Administrator can create, modify or delete user's accounts in the TOE. In particular, general information about each user can be registered in the user account.

283 c) *Management of user accounts' credential information: validity period, minimum number of different consecutive passwords (for password renewal), maximum number of unsuccessful authentication attempts, enabling/disabling X.509 certificate-based authentication, assign Certification Authorities as valid (if X.509 certificate-based authentication is enabled), re-generate the user's password.*

284 The Security Administrator can create new user accounts, configuring the password validity period, the minimum number of different consecutive passwords (for password renewal) and the maximum number of unsuccessful authentication attempts, among others..

285 The Security Administrator can also bind certain Certification Authorities as valid for the user account, selecting them from those supported by the TOE. It will restrict the certificates that can be auto-enrolled by the user.

286 Re-generating a user's password implies that the previous one becomes invalid. The new one must be communicated to the user using a secure out-of-band mechanism.

287 d) *Management of state of user's account: block/activate the user account*.

288 The Security Administrator can block a user account at will, in case a suspicious activity is detected or a potential compromise of the user's credentials is suspected. On the other hand, the Security Administrator can reactivate a previously blocked user account.

289 e) *Management of visibility conditions for each user account.*

290 The Security Administrator can establish the visibility conditions for the PI3 Access Control Policy (PI3AC Policy) enforcement.

291 f) *Management of a list of explicitly permitted critical infrastructures for each user account.*

292 The Security Administrator can establish a list of explicitly permitted critical infrastructures for the PI3 Access Control Policy (PI3AC Policy) enforcement.

293 g) *Management of supported Certification Authorities*.

294 The Security Administrator can manage the Certification Authorities that are regarded as valid (supported) inside the TOE boundaries. This configuration will delimit the Certification Authorities that can be bound to a user's account.

295 h) *Management of user's credentials, including: auto-enrol new X.509 certificates, and change password*.

296 Every user is able to manage her own credentials, including the password and the certificates with which the user can authenticate, provided that they are issued by a supported Certification Authority.

297 i) *Management of the System configuration (password quality metrics): Minimum password length, mandatory use of numbers in passwords, mandatory use of special characters in passwords*.

298 The TOE is installed with some fixed security parameters (System configuration):

299 – Minimum validity period for passwords (1 day)

300 – Maximum validity period for passwords (60 days)

301 – Maximum number of unsuccessful authentication attempts (5)

302 – Minimum number of different passwords a user has to select during consecutive password renewals (5).

303 These constraints can be made more restrictive (never less restrictive) at user account level. Therefore, a Security Administrator is allowed to make the security parameters for users more restrictive at any time.

304 The TOE also permits a Security Administrator to configure the password quality metrics for the TOE users, which include:

305 – Minimum length.

306 – Mandatory use of numbers.

307 – Mandatory use of special characters.

308 Changes in password quality metrics are made effective next time a user has to change the password, or when the Security Administrator re-generates a user's password.

309 j) *Management of the System configuration (Web Services management): certificate used by the TOE to sign the SOAP responses, users authorised to invoke the web services published by the TOE*.

310 The Security Administrator can manage information related to the Web Services façade configuration.

311 In particular, the Security Administrator can establish the X.509 certificate (in practice, the key pair) used by the TOE to sign the SOAP responses.

312 On the other hand, the Security Administrator can set the users that are authorised to invoke the services published by the TOE.