An Indra company

SIAVAL PKI

Security Target

INDEX

1 INTRODUCTION 6
1.1 IDENTIFICATION 6
1.1.1 Security Target Reference 6
1.1.2 TOE Reference 6
1.2 TOE OVERVIEW 6
1.2.1 TOE Type 6
1.2.2 Usage of the TOE 6
1.3 TOE DESCRIPTION 9
1.3.1 TOE Components 9
1.3.2 TOE Definition 10
1.3.3 TOE Configuration 13

2 CONFORMANCE CLAIMS 14
2.1 CC CONFORMANCE CLAIM 14
2.2 PP CONFORMANCE CLAIM 14
2.3 PACKAGE CONFORMANCE CLAIM 14

3 SECURITY PROBLEM DEFINITION 15
3.1 THREATS 15
3.2 ORGANIZATION SECURITY POLICIES 16
3.3 ASSUMPTIONS 16

4 SECURITY OBJECTIVES 18
4.1 SECURITY OBJECTIVES FOR THE TOE 18
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 18
4.3 RATIONALE 20
4.3.1 Security Objectives Rationale 20
4.3.2 Security Objectives Sufficiency 24
4.3.3 Conclusion 30

5 EXTENDED COMPONENTS DEFINITION 31
5.1 FAU_STG-SECURITY AUDIT EVENT STORAGE 31
5.2 CLASS FKI: SECURITY KEY INFRASTRUCTURE 32
5.2.1 Security Certificate X509 (FKI_CER) 32
5.2.2 Security Certificate Revocation List (FKI_CRL) 34
5.2.3 Security Export Data (FKI_EXP) 35

5.3 CRYPTOGRAPHIC OPERATION 36

6 SECURITY REQUIREMENTS 38
6.1 SECURITY FUNCTIONAL REQUIREMENTS 38
6.1.1 Security Audit 38
6.1.2 Roles 42
6.1.3 Access Control 43
6.1.4 Identification and Authentication 44
6.1.5 Management of security attributes 45
6.1.6 Remote Data Entry and Export 46
6.1.7 Cryptographic operations 47
6.1.8 FKI Operation 47
6.2 REQUIREMENT DEPENDENCY RATIONALE 49
6.2.1 Rationale that Dependencies Are Satisfied 49
6.3 SECURITY REQUIREMENTS RATIONALE 52
6.3.1 Security Requirements Sufficiency 54
6.4 SECURITY ASSURANCE REQUIREMENTS 56

7 TOE SUMMARY SPECIFICATIONS 57
7.1 ACCESS CONTROL 57
7.2 KEY MANAGEMENT 58
7.3 MANAGEMENT OF THE ISSUANCE OF CERTIFICATES AND CRLS 58
7.4 DATA TRANSMISSION SECURITY 58
7.5 AUDIT DATA 59

8 TOE ACCESS CONTROL POLICY 61

9 NORMATIVE REFERENCES 62

10 ACRONYMS AND TERMINOLOGY 63

List of Tables

Table 1: Security Target Reference 6

Table 2: TOE Reference 6

Table 3: Relationship of Security Objectives for the TOE to Threats 21

Table 4: Relationship of Security Objectives for the Environment to Threats 22

Table 5: Relationship of Organizational Security Policies to Security Objectives 22

Table 6: Relationship of Assumptions to IT Security Objectives 23

Table 7: Auditable Events and Audit Data 42

Table 8: Authorized Roles for Management of Security Functions Behavior 43

Table 9: Summary of Security Functional Requirements Dependencies 52

Table 10: Security Functional Requirements Related to Security Objectives 54

Table 11: Assurance Requirements 56

List of Figures

Figure 1: Logical TOE architecture 11

Figure 2: TOE Configuration..... 13

1 Introduction

1.1 Identification

This Security Target describes the objectives and safety requirements of SIAVAL PKI. The specifications are consistent with Common Criteria for Information Technology Security Evaluation v3.1 R5.

1.1.1 Security Target Reference

TITLE	VERSION	AUTHOR	DATE
SIAVAL PKI – Security Target	5.0	SIA	23/03/2022

Table 1: Security Target Reference

1.1.2 TOE Reference

TOE IDENTIFICATION	SIAVAL PKI
VERSION	1
AUTHOR	Sistemas Informáticos Abiertos S.A.U. (SIA)
CC CONFORMANCE	Common Criteria for Information Technology Security Evaluation v3.1 R5
ASSURANCE LEVEL	EAL 4 + ALC_FLR.1

Table 2: TOE Reference

1.2 TOE Overview

1.2.1 TOE Type

SIAVAL PKI as a Certification Authority is the certificate management solution of the SIAVAL product family, offering a complete solution for the implementation of certification authorities and the management of the certificate life cycle, covering the main use cases associated with this technology. It is a modular, highly scalable, and flexible product, based on standards and which supports the management of multiple hierarchical certification authorities.

1.2.2 Usage of the TOE

The solution allows to comply with the most demanding worldwide standards for the use of PKI technology, such as ETSI/eIDAS or WebTrust; mandatory standards in many of the services that require this type of technology.

The set of components that make up SIAVAL PKI makes it possible to issue certificates as well as manage their states throughout their life cycle, their publication in different repositories as well as the issuance of CRLs in order to determine the certificates that have been revoked from the CA.

A hierarchy of CA's can be established according to the needs of the system, allowing different profiles to be established for each CA so that certificates can be issued for different purposes.

Control of their signature keys is established at all times, ensuring the issuance of certificates by the CA as well as from their subordinate CA's.

The way to interact with the TOE is through interfaces through which certificates will be requested to be issued based on the profiles stored in the system.

These interfaces are as follows:

- **WebServices Interfaces:** The JAX-WS 2.0 web service interface is used to access CA functions remotely through HTTPS and client authentication.
- **AdminWeb:** Web administration console from which the use of the TOE is managed and the management of users, roles and profiles of certificates and certificate revocation lists is carried out.
- **HealthCheck:** Service for monitoring the status of the TOE.

The most common use cases that can be solved with SIAVAL PKI are:

- **eIDAS Providers.** SIAVAL PKI serves as an essential basis for the provision of qualified and reliable services for the issuance of signature certificates, seals, time stamps and associated profiles, according to the ETSI EN 319 4xx family of standards.
- **ICAO eMRTD/ePassport**, allowing the implementation of the infrastructure for issuing e-passport certificates.
- **SSL Certificates for websites and components**. Allows the implementation of certification authorities for the issuance of server certificates, including the basis for the establishment of browser-trusted web server certificate issuance services according to CA/Browser Forum.
- **IoT-Internet of Things**, for authenticated, integrated and reliable communication between devices.
- **Integration with MDM/UEM systems**, by directly integrating with leading manufacturers of mobile device management technology to automate the rolling out of certificates to multi-use devices.
- **Private Networks /VPN**, to establish trusted environments for networks, remote access clients and VPNs by issuing digital certificates.
- **User authentication**, including active directory services or cloud-based applications, from desktops or mobile devices.
- **Secure email**, with advanced key management capabilities for email encryption.

1.2.2.1 Major Security Features of the TOE

The safety features of the TOE are summarized in:

- **Access Control**:

  Access control is established for the operations performed in the TOE so that only authorized users can perform the operations for which they have been authorized.

  Only the HealthCheck service does not establish user access control but performs IP access control to validate the origin of the requests.

- **Key Management**: The private keys of the CAs will reside in a cryptographic module and the TSF will make use of them for the issuance of certificates and CRLs, invoking the signature operation on the device.

  The public keys are stored in x509 certificates and protected in integrity.

- **Management of the issuance of certificates and CRLs**: Several CA's can be managed by establishing a hierarchy among them, so that a Root CA and subordinate CA's can be established to issue for example certificates with different purposes, personal signature certificates, SSL/TLS Web certificates, etc.

  Certificates and signed CRLs are generated, making it possible to request certificates through CSR using a mechanism such as PKCS # 10 or CRMF.

  Profiles and configurations are established for the issuance of certificates and generation of CRLs, so that it is possible to establish your own characteristics depending on the configuration of the profile.

  It enables the publication of certificates and CRLs in different repositories as well as the recovery of these certificates and CRLs from the TOE itself.

- **Transmission Data security:**

  The User Keys will always be exported in keystores and certificates and CRLs will always be issued in a way that preserves their integrity.

- **Audit Data:** Audit trail is recorded for all operations performed by users in the system.

  A value calculated by the TSF will be added so that the integrity of the contained data can be checked.

1.2.2.2 Hardware/Software/Firmware Elements that are not part of the TOE but are necessary for its proper functioning

The following software and hardware components are considered external to the TOE, although they are necessary for its proper functioning:

- Machine with operating system, application server and other management utilities pre-installed, on which the TOE software is installed and delivered in appliance mode.

  The TOE runs on a machine in Appliance format that ensures its integrity and proper functioning.

- Operating system: The TOE is independent of the operating system where it is executed; it only needs to be able to run a Java virtual machine that will be running on that operating system. The TOE does not use any characteristic or security functionality of the operating system that requires the use of a specific version of the same.

- Application Server: The TOE software is a J2EE application that must be run on an application server with EJB (Enterprise Java Beans) support.

- Cryptographic module (HSM): Cryptographic hardware that performs the cryptographic operations carried out by the TOE. Indicate that the HSM may reside in the appliance or outside it if a secure network connection HSM is available.

  HSM: The interaction with the TOE is done through the PKCS#11 interface of each HSM manufacturer.

- Database for the storage of the system's operating configuration, work data, operation traces, etc. The TOE does not require any special security features or functionality of the database that require the use of any particular model or version of the database. Only that the communication is established trough SSL.

  This database can be configured inside the physical appliance where the TOE resides or outside it by establishing a secure communications channel.

- Registration authority (RA): Registration authority or client software that does the RA functionality that through the interfaces of the TOE invokes the issuance of certificates. This software is not necessary for the operation of the TOE itself, but it is necessary to be able to interact with it through its WebServices interface.

- NTP Server: NTP service for time synchronization through a reliable time source.

Minimum Supported Versions:
- OS: CentOS Release 7.x
- Java Runtime Environment: OpenJDK 1.8.x
- Application Server: Wildfly 12.x
- HSM: Luna PCI-E Cryptographic Module Luna PCI 6 or 7
- Database: PostgreSQL 12.x

1.3 TOE Description

SIAVAL PKI comprises all the security functions required by a Certification Authority, allowing the issuance of certificates and CRLs, the management of the life cycle of these certificates and the capacity to provide information about the revocation status so that from a VA its status can be verified.

1.3.1 TOE Components

The TOE SIAVAL PKI consists of a set of modules based on the open source solution of EJBCA in its Community version where other proprietary modules of the SIAVAL family have been incorporated, such as the component for the protection of audit logs and integration with the SIAVAL VA.

The modules that make up the TOE SIAVAL PKI are listed below:

- Administration Console AdminWeb for user management, roles, certificate profiles, certificate management, etc.
- Core EJB module where the system functionality is implemented called EJBCore.

- WebServices Interface module; offers the services of the CA through SOAP web services, called EJB-WS.
- Certificate and CRL Publisher Module, Certificate Status Publisher Module and SIAVAL Certificate Status Publisher Module are all included in the module called Publishers.
- SIAVAL Audit trail generation/protection module called LogIntegrity.
- PKCS#11 Module that communicates with the hardware cryptographic module (HSM).
- SoftCrypto Module for cryptographic operations made for the TOE.
- HealthCheck Module for monitoring the status of the TOE.

1.3.2 TOE Definition

1.3.2.1 Physical scope

The TOE is software where all components are included and supplied in a single file type ear.

- sia_ca.ear, version 1

The software is delivered to the end user installed on a hardware machine as an appliance, with the operating system, application server and other necessary utilities and interfaces previously installed.

Along with the TOE software, a set of manuals in .pdf format is provided, which describe how to configure and operate each of the components that constitute it as well as its operating environment.

These manuals are delivered to the customer by the technicians in charge of commissioning the appliance where the TOE is installed. The physical delivery format is agreed with the customer, delivering said manuals on a CD, USB memory or copy on a device provided by the customer.

List of TOE manuals:

- *SIAVAL PKI - Manual de Operaciones*, version 1.2, 16/12/2021: Operations manual for SIAVAL PKI roles in pdf format.
- *SIAVAL PKI - Manual de Configuración Segura*, version 1.3, 23/03/2022: Secure configuration for compliance of common criteria certification in pdf format.
- SIAVAL PKI - Manual de uso Servicios Web, version 1.1, 09/12/2021: User manual for use the Web Services interface in pdf format.

1.3.2.2 Logical Scope

The TOE is a set of components that make up the solution, all of them running on an application server but in a modular way.

The logical components included in the TOE are:

- **SIAVAL PKI AdminWeb**: Administration Console Web.
- **EJBCore Module:** Core System functional module.
- **WebServices Interface:** Provides access to the TOE through a WebServices interface.
- **Certificate and CRLs publisher module:** Module that is in charge of publishing the certificates and CRLs issued by the TOE.

- **Certificate status publisher module**: Module that is responsible for publishing the status of certificates.
    - **SIAVAL Certificate status publisher module**: Module that is responsible for publishing the status of certificates for SIAVAL VA.
- **SIAVAL Audit records generation and protection module:** Module called LogIntegrity that records the security events of the system so that they are protected in integrity.
- **PKCS#11 module:** Module used for communication between the TOE and the cryptographic module. The TOE uses the PKCS11 standard to communicate with the customer that each manufacturer of the cryptographic module provides in order to interact with it.
- **SoftCrypto module:** Module for cryptographic operations made by the TOE to protect assets that will be stored in the database, such as passwords, activation codes or users' key pairs.
- **HealthCheck Interface:** Provides system status of the TOE.

The following illustration represents the logical architecture of the components that make up the complete solution, distinguishing between those that belong to the TOE and those components that are not part of the TOE and are external to it but are necessary for its proper functioning:

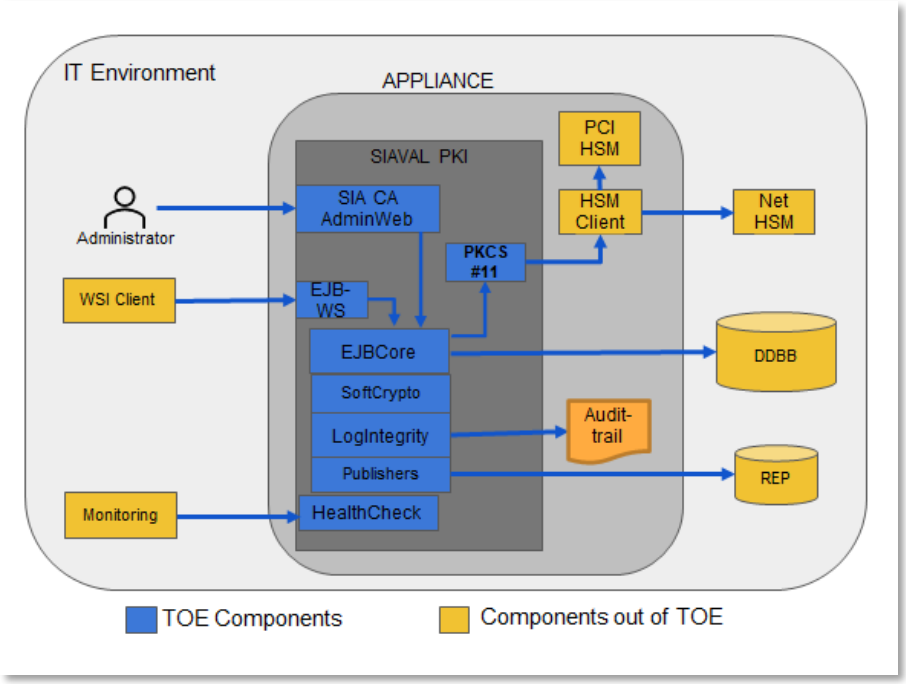

Figure 1: Logical TOE architecture

1.3.2.3 Security Functions

The main safety functions of the TOE are:

1.3.2.3.1 Access Control

Access to the functionalities offered both through the web services and the administration console is carried out under the access control established by the authentication requirement by means of

certificates. In this way, a strong identification is established between the clients that use the services and the TOE uniquely authenticating the applications requesting the TOE services.

Likewise, users are associated with roles that determinate the authorisation of access to each of the system's resources, so that users can only carry out those operations that access the resources determined by their assigned privileges.

1.3.2.3.2 Key Management

The keys of the CAs will be stored in a cryptographic module and the TOE will invoke the cryptographic operations so that the electronic signatures made for the issuance of certificates and CRLs by the CA are assured.

The user public keys are stored in x509 certificates signed with CA private key protected in integrity.

1.3.2.3.3 Management of the issue of certificates and crls

Each CA can manage the certificate profiles to be issued, as well as the issue of CRLs with the revocation of the certificates. In this way, it will have absolute control over the type of certificate to be issued by each CA to each user for different purposes, such as personal signature certificates, SSL/TLS Web certificates, etc.

The certificates and CRLs issued comply with the X509 and RFC 5280 standards in such a way as to ensure the compatibility of these certificates with other certificate management systems and the electronic signature performed by the TOE.

The system has the necessary mechanisms to publish the revocation statuses of the certificates through the publication of CRLs.

1.3.2.3.4 Data transmission security

The users' keys will be transmitted securely to the applicant, these keys will always be exported in key stores format.

Likewise, the certificates and CRLs will be issued digitally signed and protected in integrity.

1.3.2.3.5 Audit Data

The system will record each operation carried out by the users, identifying who originated the process at the date and time, and therefore the security operations carried out in the system will be recorded.

The TOE can calculate a cryptographic value that is added to the audit data so that is integrity can be verified by a process which is out of the TOE boundary.

1.3.3 TOE Configuration

Although the TOE supports other platforms, the tests to carry out the evaluation of the TOE are performed on a specific platform that has the following significant characteristics:

- **Hardware**:
  - **Machine appliance where the TOE resides**: Dell PowerEdge with Intel(R) Xeon(R)
  - **HSM**: LUNA PCI-E Cryptographic Module. Luna PCI 7
  - **Machine with components external to the TOE**: Virtual Machine with Operating System Windows 2012 R2.
- **Software**:
  - **Operating system on the TOE server**: CentOS release 7.8.2003 (Core) of 64 bits.
  - **Application server**: WildFly 12
  - **Database**: PostgreSQL 12
  - **HSM Client**: Luna PCI Client. 7
  - **Java Runtime Environment**: OpenJDK 1.8.0_252
  - **TOE**: SIAVAL PKI 1

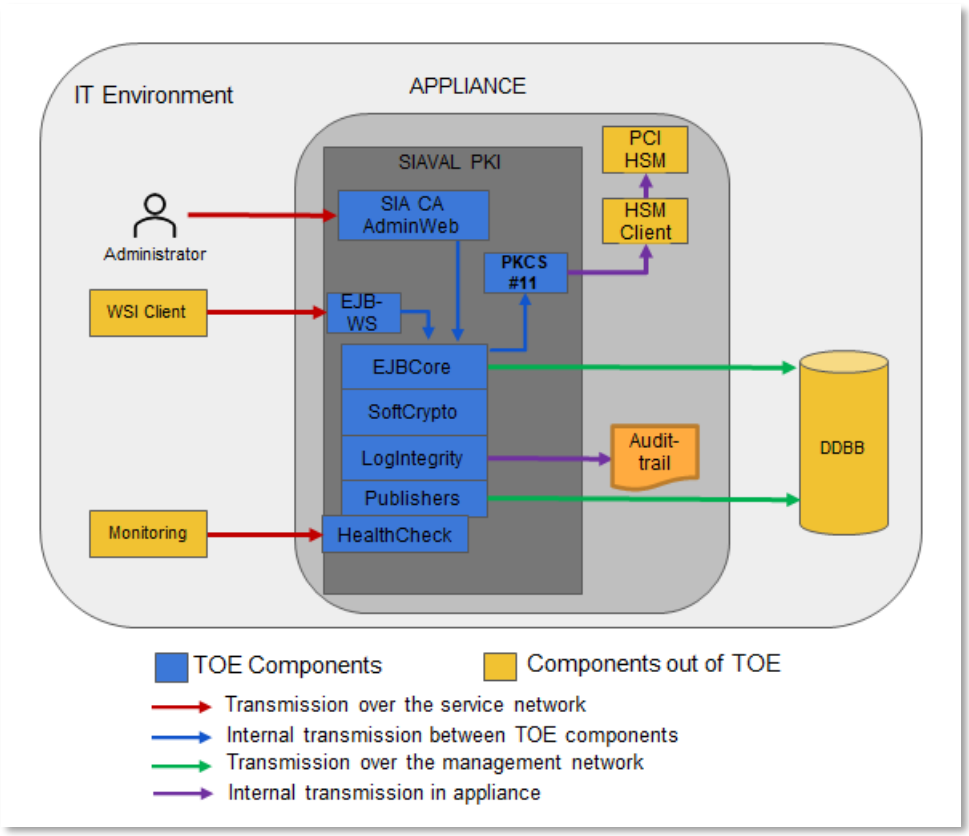

Figure 2: TOE Configuration

2 Conformance Claims

2.1 CC conformance claim

The TOE is declared compliant with Parts 2 and 3 of the Common Criteria for Information Technology Security Evaluation, v3.1 Revision 5.

- Security Functional Requirements Part 2 of Common Criteria v3.1 R5 extended.
- Security Assurance Requirements Part 3 of Common Criteria v3.1 R5 conformant for Certification Level EAL4 + ALC_FLR.1.

The evaluation methodology is Common Methodology for Information Technology Security Evaluation CEM v3.1 R5.

2.2 PP conformance claim

The SIAVAL PKI Security Target does not conform to any Protection Profile.

2.3 Package conformance claim

This SIAVAL PKI Security Target claims conformance to assurance package EAL4 augmented with ALC_FLR.1.

3 Security Problem Definition

This section identifies the elements that allow the TOE security problem to be defined.

3.1 Threats

The threats are organized into three categories: authorized users, system and external attacks.

Authorized users: The agents of the following threats are authorized users. The assets that are compromised are the certificates, CRLs, the TOE itself and the audit trail.

- **T.Administrative errors of omission: Authorized users** fail to perform some function essential to security resulting in a lack of ***integrity*** of the certificates and CRLs.
- **T.Authorized users commit errors or hostile actions:** An **authorized user** commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur, resulting in a lack of ***integrity*** of the system assets.
- **T.User abuses authorization to collect and/or send data:** User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data, resulting in a lack of ***confidentiality*** of the system assets.
- **T.User error makes data inaccessible:** Authorized user accidentally deletes user data rendering user data ***inaccessible***.
- **T.Sender denies sending information:** The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction. Threat agent is an authorized user, and this adverse action can be reduced the authenticity of audit trail.

System

- **T.Malicious code exploitation:** An authorized user, TOE itself, or hacker downloads and executes malicious code, which causes abnormal processes that violate the ***integrity***, or ***confidentiality*** of the system assets. Threat agent could be an authorized user, TOE itself, or an unauthorized user. Adverse actions can compromise the security of the TOE and / or trusted party systems that depend on PKI objects, such as the integrity of certificates and CRLs.
- **T.Message content modification:** A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient causing a breach of ***confidentiality*** and ***integrity*** of system assets. Threat agent is an unauthorized user. Adverse actions can compromise the security of the TOE and / or trusted party systems that depend on PKI objects, due to loss of integrity of certificates and CRLs.

External Attacks

- **T.Hacker gains Access:** A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of ***integrity*** or ***confidentiality***. Threat agent is the unauthorized user. Adverse actions may compromise the security of the TOE and / or

trusted party systems that rely on PKI objects, due to loss of integrity of certificates and CRLs.

- **T.Hacker physical Access:** A hacker physically interacts with the system to exploit vulnerabilities in the physical environment. Threat agent is the unauthorized user and adverse actions may compromise the security of the TOE and / or trusted party systems that rely on PKI objects, due to loss of integrity of certificates and CRLs.
- **T.Hacker modifies certificates or crls:** A hacker modifies the certificates or crls issued by the CA. Threat agent is the unauthorized user and adverse actions may compromise the security of the TOE and / or trusted party systems that rely on PKI objects, due to loss of integrity of certificates and CRLs.

3.2 Organization Security Policies

- **P.Authorized use of information:** Information shall be used only for its authorized purpose(s).
- **P.Cryptography:** FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

3.3 Assumptions

- **A.Auditors Review Audit Logs:** Audit logs are required for security-relevant events and must be reviewed by the Auditors.
- **A.Authentication Data Management:** An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.).
- **A.Competent Authorized Users:** Competent and trustworthy authorized users will be assigned to manage the TOE and the security of the information it contains. Every user shall follow the guidance provided for the TOE.
- **A.CPS:** All authorized users are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
- **A.Disposal of Authentication Data:** Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
- **A.Sufficient backup and restore:** Periodic backups will be carried out ensuring that the system can be restored to a safe state, recovering it from possible malicious code attacks as well as hardware errors or loss of logical data.
- **A.Communications Protection:** The system is adequately physically protected against loss of communications and security configuration i.e., availability of communications. The system will create the channels through which the TOE will send/receive data. The management network interface shall be configured in such a way that it is isolated from the TOE access service network interface, so that it is isolated and protected from unauthorized access.
- **A.Physical Protection:** The hardware and software of the operating environment where the TOE is operated including HSM, Database and physical appliance where the TOE is installed will be protected against physical modifications and unauthorized access.

- **A.Time stamps:** The system will have a secure time source to provide the TOE with an accurate and reliable timestamp.
- **A.Validation of security function:** Software, hardware and firmware that is not part of the TOE will be monitored to guarantee the correct functioning.
- **A.React to detected attacks:** System on which the TOE is deployed, will implement automated notification (or other responses) to the discovered attacks.

4 Security Objectives

This section identifies and defines the security objectives for the TOE and for the operating environment. The security objectives reflect the intention to counteract the identified threats, as well as to comply with the organization's security policies and assumptions.

4.1 Security Objectives for the TOE

- **O.Certificates:** The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.
- **O.Non-repudiation:** Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.
- **O.Data import/export:** Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
- **O.Individual accountability and audit records:** Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action. The analysis and consultation of audit data is not part of the scope of the objective.
- **O.Limitation of administrative Access:** Design administrative functions so that authorized users do not automatically have access to user objects, except for necessary exceptions. Control access to the TOE by authorized users who operate the TOE.
- **O.Protect stored audit records:** Include the HMAC compute value in the audit logs to provide a mechanism to detect data modification and thus ensure accountability for user actions.
- **O.Restrict actions before authentication:** Restrict the actions a user may perform before the TOE authenticates the identity of the user.
- **O.Configuration Management:** Configuration management must be implemented for the issuance of certificates and CRLs.
- **O.Maintain user attributes:** Maintain a set of security attributes (which may include role membership. Access privileges, etc.) associated with individual users.
- **O.Security roles:** Maintain security-relevant roles and the association of users with those roles.

4.2 Security Objectives for the Environment

- **OE.Authorized Users guidance documentation:** Avoid authorized users errors by providing adequate documentation on securely installing, configuring and operating the TOE.
- **OE.Auditors Review Audit Logs:** Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.
- **OE.Authentication Data Management:** Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)
- **OE.Competent Authorized Users:** Provide capable management of the TOE by assigning competent and trustworthy authorized users to manage the TOE and the security of the information it contains.

- **OE.CPS:** All authorized users shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.
- **OE.Cryptographic functions:** A validated cryptographic module must be available in the environment so that the TOE can invoke cryptographic operations on it. (Validated is defined as FIPS 140-2 validated.)

  The approved cryptographic algorithms must be configured in the cryptographic module in compliance with the established security policy.
- **OE.Disposal of Authentication Data:** Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).
- **OE.Physical Protection:** Those responsible for the TOE and the operating environment must ensure that the equipment, including the machine where the TOE resides, HSM, the database and the management network that communicates these equipment, are protected against physical attacks and unauthorized access that may compromise system security.
- **OE.Sufficient backup storage and effective restoration:** Provide sufficient backup storage including audit logs and effective restoration to ensure that the system can be recreated. Recover to a viable state after malicious code is introduced and damage occurs, that state must be free from the original malicious code.
- **OE.Trusted Path:** There must be two different trust channels, a management channel and a service channel, the service channel will be used to access the TOE services and the management channel used by the elements of the operating environment, such as the database, the HSM and access to the machine where the TOE resides for the purpose of administration or auditing.

  This management network, separate from the service network, must not be accessible from outside the operating environment, preventing it from being attacked by external elements.
- **OE.Validation of security function:** Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.
- **OE.Detect modifications of software updates and backup data:** Provide integrity protection to detect modifications to software and backup data. Incorporate malicious code prevention procedures and mechanisms.
- **OE.React to detected attacks:** Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.
- **OE.Security-relevant configuration management:** Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies. Among these settings, the key and settings related to the HMAC calculation for the audit logs will already be generated and configured to be used by the TOE from its installation by the manufacturer on the appliance.
- **OE.User authorization management:** Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.
- **OE.Time stamps:** Provide time stamps to ensure that the sequencing of events can be verified.

4.3 Rationale

This section includes the rationale for the functional and assurance requirements specified for the TOE. The rationale is based on specified objectives, threats, assumptions, and policies.

4.3.1 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, policies, or assumptions. The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy or assumption is covered by at least one security objective.

Table 3 maps security objectives for the TOE to threats.

Table 4 maps security objectives for the environment to threats.

Table 5 maps the organizational security policies to security objectives.

Table 6 maps assumptions to IT security objectives, listing which objectives each assumption helps to cover.

SECURITY OBJECTIVE	THREAT
O.Certificates	T.Authorized Users commit errors or hostile actions T.Hacker modifies certificates or crls
O.Data import/export	T.Message content modification
O.Individual accountability and audit records	T.Administrative errors of omission, T.Hacker gains Access, T.Authorized Users commit errors or hostile actions, T.User abuses authorization to collect and/or send data
O.Limitation of administrative Access	T.Authorized Users commit errors or hostile actions
O.Maintain user attributes	T.Authorized Users commit errors or hostile actions
O.Non-repudiation	T.Sender denies sending information

O.Protect stored audit records	T.Authorized Users commit errors or hostile actions
O.Restrict actions before authentication	T.Hacker gains access, T.Authorized Users commit errors or hostile actions
O.Configuration Management	T.Authorized Users commit errors or hostile actions
O.Security roles	T.Authorized Users commit errors or hostile actions

Table 3: Relationship of Security Objectives for the TOE to Threats

SECURITY OBJECTIVE FOR ENVIRONMENT	THREAT
OE.Authorized Users guidance documentation	T.Authorized Users commit errors or hostile actions
OE.Auditors Review Audit Logs	T.Authorized Users commit errors or hostile actions T.Hacker gains access
OE.Authentication Data Management	T.Hacker gains access
OE.Competent Authorized Users	T.Authorized Users commit errors or hostile actions
OE.CPS	T.Administrative errors of omission
OE.Cryptographic functions	T.Hacker modifies certificates or crls
OE.Disposal of Authentication Data	T.Authorized Users commit errors or hostile actions
OE.Physical Protection	T.Hacker physical access
OE.Sufficient backup storage and effective restoration	T.User error makes data inaccessible T.Malicious code exploitation

OE.Trusted Path	T.Hacker gains access, T.Message content modification
OE.Validation of security function	T.Malicious code exploitation, T.Authorized Users commit errors or hostile actions
OE.Detect modifications of software updates and backup data	T.User error makes data inaccessible, T.Authorized Users commit errors or hostile actions T.Malicious code exploitation
OE.React to detected attacks	T.Hacker gains access
OE.Security-relevant configuration management	T.Administrative errors of omission
OE.User authorization management	T.Administrative errors of omission
OE.Time stamps	T.Authorized Users commit errors or hostile actions

Table 4: Relationship of Security Objectives for the Environment to Threats

SECURITY POLICY	OBJECTIVE
P.Authorized use of information	OE.Auditors review audit logs O.Maintain user attributes O.Restrict actions before authentication O.Security roles OE.User authorization management
P.Cryptography	OE.Cryptographic functions

Table 5: Relationship of Organizational Security Policies to Security Objectives

ASSUMPTION	SECURITY OBJECTIVE FOR ENVIRONMENT
A.Auditors Review Audit Logs	OE.Auditors Review Audit Logs
A.Authentication Data Management	OE.Authentication Data Management
A.Communications Protection	OE.Trusted Path
A.Competent Authorized Users	OE.Competent Authorized Users, OE.Security-relevant configuration management, OE.User authorization management OE.Authorized Users guidance documentation
A.CPS	OE.CPS, OE.Security-relevant configuration management, OE.User authorization management
A.Disposal of Authentication Data	OE.Disposal of Authentication Data
A.Sufficient backup and restore	OE.Detect modifications of software updates and backup data OE.Sufficient backup storage and effective restoration
A.Physical Protection	OE.Physical Protection
A.Time stamps	OE.Time stamps
A.Validation of security function	OE.Validation of security function
A.React to detected attacks	OE.React to detected attacks

Table 6: Relationship of Assumptions to IT Security Objectives

4.3.2 Security Objectives Sufficiency

The following discussions provide information regarding:

Why the identified security objectives provide for effective countermeasures to the threats;
Why the identified security objectives provide complete coverage of each organizational security policy;
Why the identified security objectives uphold each assumption.

4.3.2.1 Threats and Objectives Sufficiency

4.3.2.1.1 Authorized Users

T.Administrative errors of omission addresses errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application. It is countered by:

OE.CPS provides authorized users with information regarding the policies and practices used by the system. Providing this information ensures that these authorized users of the system are aware of their responsibilities, thus reducing the likelihood that they will fail to perform a security-critical operation.

O.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that fail to perform security-critical operations so they can be held accountable.

The analysis of the audit data will be carried out by auditors through the mechanisms that the operating environment establishes to access said data. The analysis and consultation of audit data is not part of the scope of the TOE.

OE.Security-relevant configuration management ensures that system security policy data and enforcement functions, and other security-relevant configuration data are managed and updated. This ensures that they are consistent with organizational security policies and that all changes are properly tracked and implemented.

OE.User authorization management ensures the correct configuration and management of the policy established for access control.

T.User abuses authorization to collect and/or send data addresses the situation where an authorized user abuses granted authorizations by browsing files in order to collect data and/or violates export control policy by sending data to a recipient who is not authorized to receive the data.

It is countered by:

O.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This audit records will expose users who abuse their authorized to collect and/or send data.

The analysis of the audit data will be carried out by auditors through the mechanisms that the operating environment establishes to access said data. The analysis and consultation of audit data is not part of the scope of the TOE.

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user data is inaccessible. Examples include the following:

User accidentally deletes data by striking the wrong key on the keyboard or by striking the enter key as an automatic response.

User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes user data.

User misunderstands a system command and issues a command that unintentionally deletes user data.

It is countered by:

> **OE.Sufficient backup storage and effective restoration** ensures that there is sufficient backup storage and effective restoration to recreate the system, when required. This ensures that user data is available from backup, even if the current copy is accidentally deleted.
>
> **OE.Detect modifications of software updates and backup data** ensures that if the backup components have been modified, that it is detected. If modifications of backup data cannot be detected, the backup copy is not a reliable source for restoration of user data.

T.Authorized Users commit errors or hostile actions addresses:
Errors committed by administrative personnel that directly compromise organizational security objectives, change the technical security policy enforced by the system or application, or malicious obstruction by administrative personnel of organizational security objectives or modification of the system's configuration to allow security violations to occur.

It is countered by:

> **OE.Competent Authorized Users** ensures that users are capable of maintaining effective security practices. This reduces the likelihood that they will commit errors.
>
> **OE.Authorized Users guidance documentation** which avoids administrative personnel errors by providing adequate guidance.
>
> **OE.Auditors Review Audit Logs** through which erroneous or malicious operations can be detected.
>
> **O.Certificates** ensures that certificates, certificate revocation lists, and certificate status information are valid. The validation of information provided by administrators that is to be included in certificates helps to prevent improperly entered information from appearing in certificates.
>
> **OE.Detect modifications of software updates and backup data** ensures that if the backup components or software updates have been modified, that it is detected.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that perform inappropriate operations so they can be held accountable.

The analysis of the audit data will be carried out by auditors through the mechanisms that the operating environment establishes to access said data. The analysis and consultation of audit data is not part of the scope of the TOE.

O.Limitation of administrative access. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific. Limiting the set of operations that a user may perform limits the damage that a user may cause.

O.Maintain user attributes. Maintains a set of security attributes (which may include group membership, access rights, etc.) associated with individual users in addition to user identity. This prevents users from performing operations that they are not authorized to perform.

O.Protect stored audit records ensures that audit logs contain an HMAC value that enables detection of unauthorized modification or removal to provide traceability of user actions.

O.Restrict actions before authentication ensures that only a limited set of actions may be performed before a user is authenticated.

O.Security roles ensures that security-relevant roles are specified and that users are assigned to one (or more) of the defined roles. This prevents users from performing operations that they are not authorized to perform.

OE.Time stamps ensures that time stamps are provided to verify a sequence of events. This allows the reconstruction of a timeline of events when performing an audit review.

OE.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as monitoring and integrity checks.

OE.Disposal of Authentication Data ensures that users who should not have access can access the TOE.

O.Configuration Management ensures that the configuration for the issuance of certificates and crls has been established according to the established policies.

T.Sender denies sending information addresses the situation where the sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

It is countered by:

O.Non-repudiation which ensures that the sender/originator of a message cannot successfully deny sending the message to the recipient. Ensuring the sender of the message ensures the record in the audit trail of the sender who requested the operation.

4.3.2.1.2 System

T.Malicious code exploitation addresses the threat where an authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. The execution of malicious code is done through a triggering event.

It is countered by:

> **OE.Sufficient backup storage and effective restoration** ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.
>
> **OE.Detect modifications of software updates and backup data** ensures that modifications in software updates are detected, in this way avoid installing software with malicious code.
>
> **OE.Validation of security function**. Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.

T.Message content modification addresses the situation where a hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes.
It is countered by:

> **O.Data Import/Export** protects data when being transmitted to or from the TOE. Protection of data in transit permits the TOE or the external user to detect modified messages, message replay, or fraudulent messages.
>
> **OE.Trusted path** ensures that a trusted path is established between the user and the system. The trusted path protects messages from interception or modification by a hacker.

4.3.2.1.3 External Attacks

T.Hacker gains access addresses:
Weak system access control mechanisms or user attributes
Weak implementation methods of the system access control
Vulnerabilities found in system or application code that allow a hacker to break into a system undetected.

It is countered by:

> **O.Restrict actions before authentication** ensures that only a limited set of actions may be performed before a user is authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms from performing security-relevant operations.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This allows for the detection of unauthorized activity. Once detected, the damage resulting from such activity can be eliminated or mitigated.
>
> The analysis of the audit data will be carried out by auditors through the mechanisms that the operating environment establishes to access said data. The analysis and consultation of audit data is not part of the scope of the TOE.
>
> **OE.React to detected attacks** ensures that automated notification or other reactions to the TSFdiscovered attacks is implemented in an effort to identify attacks and to create an attack deterrent. This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.

OE.Trusted path ensures that a trusted path is established between the user and the system. The trusted path is used to protect authentication data, thus reducing the likelihood that a hacker can masquerade as an authorized user.

OE.Auditors Review Audit Logs through which unauthorized access can be detected.

OE.Authentication Data Management ensures the updating of access credentials making their use difficult by third parties.

T.Hacker physical access addresses the threat where an individual exploits physical security weaknesses to gain physical control of system components.

It is countered by:

OE.Physical Protection ensures that physical access controls are sufficient to thwart a physical attack on system components, including the machine where the TOE resides, HSM, the database and the management network that communicates these equipment.
T.Hacker modifies certificates or crls addresses the threat where an individual modifies the certificates or crls in such a way that these modifications are not detected, evidencing the weakness of the strength of the certificates or crls issued.

It is countered by:

O.Certificates ensures the issuance of certificates and crls according to X509 and RFC5280 standard signed by a FIPS140-2 validated cryptographic device.

OE.Cryptographic functions ensures that the cryptographic device used by the TOE to perform the signature during the certificate and crls issuance process is configured to comply with FIPS140-2.

4.3.2.2 Policies and Objectives Sufficiency

P.Authorized use of information establishes that information is used only for its authorized purpose(s). This is addressed by the following objectives: **O.Maintain user attributes**, **O.Restrict actions before authentication**, **O.Security roles**, **OE.User authorization management and OE.Auditors review audit logs**. **O.Restrict actions before authentication** ensures that the capability to perform security-relevant operations is limited to those who have been authorized to perform those operations. **O.Maintain user attributes**, **O.Security roles**, and **OE.User authorization management** ensure that users are only authorized to perform those operations that are necessary to perform their jobs. Finally, **OE.Auditors review audit logs** deters users from misusing the authorizations they have been provided.

P.Cryptography establishes that accepted cryptographic standards and operations shall be used in the configuration of the cryptographic module. This is addressed by **OE.Cryptographic functions** which ensures that such standards are used.

4.3.2.3 Assumptions and Objectives Sufficiency

A.Auditors Review Audit Logs establishes that audit logs are necessary for security-relevant events and that they must be reviewed by auditors. This is addressed by **OE.Auditors Review Audit Logs**, which ensures that security-relevant events recorded in audit logs are reviewed by auditors.

A.Authentication Data Management establishes that management of user authentication data is external to the TOE. This is addressed by **OE.Authentication Data Management**, which ensures that users modify their authentication data in accordance with appropriate security policy.

A.Competent Authorized Users establishes that security of the TOE is dependent upon those that manage it. This is addressed by **OE.Competent Authorized Users**, **OE.Security-relevant configuration management, OE.User authorization management and OE.Authorized Users guidance documentation. OE.Competent Authorized Users** ensures that the system managers will be competent and trustworthy in its administration. **OE.Security-relevant configuration management** ensures that system security policy data is updated and consistent with oganizational security policies. **OE.User authorization management** ensures that user authorization data is consistent with organizational security and personnel policies. Finally, **OE.Authorized Users guidance documentation** ensures that users errors will be avoided due to the adequate documentation.

A.CPS establishes that Authorized Users are familiar with the CP and CPS under which the TOE is operated. This is addressed by **OE.CPS**, which ensures that authorized users are familiar with the CP and CPS under which the TOE is operated.

A.Disposal of Authentication Data establishes that users shall not retain access to the system after their authorization has been removed. This is addressed by **OE.Disposal of Authentication Data**, which ensures that access to the system will be denied after a user's privileges have been removed.

A.Sufficient backup and restore: establishes that periodic backup copies will be made ensuring that the system can be restored to a safe state, recovering it from possible attacks by malicious code as well as hardware errors or loss of logical data. This is addressed by **OE.Detect modifications of software updates and backup data** and **OE.Sufficient backup storage and effective restoration,** which ensures that the proper performance of backups and restoration of the system.

A.Communications Protection establishes that the communications infrastructure is outside the TOE. This is addressed by **OE.Trusted Path**, which ensures that adequate protections are afforded the necessary communications infrastructure.

A.Physical Protection establishes that the physical modification of the appliance where the TOE is installed and its operating environment, including HSM and the database, will compromise the security of the system. This issue is addressed by OE.Physical Protection, which ensures that adequate physical protection will be provided.

A.Time stamps: establishes that the system will have a secure time source to provide the TOE with an accurate and reliable timestamp. This is addressed by **OE.Time stamps** that ensure that a secure and reliable time source will be available through which the system can synchronize its time and thus trust the times recorded in the audit logs.

A.Validation of security function: establishes that the system will be monitored to guarantee the proper functioning of hardware software and firmware. This is addressed by **OE.Validation of security function**.

A.React to detected attacks: establishes that the system will implement automated notification (or other responses) to the discovered attacks. This is addressed by **OE.React to detected attacks.**

4.3.3 Conclusion

As shown in the previous sections, all threats are mitigated by one or more security objectives, as is the case with each policy and hypothesis, and have their corresponding objectives for their fulfilment, and that all the objectives established are necessary to provide a solution to the security problem.

5 Extended Components Definition

Extended components defined in this ST.

5.1 FAU_STG-Security audit event storage

Family Behaviour

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

Rationale:

We extend the family FAU_STG: Security audit event storage defined in Part 2: Security functional components of Common Criteria v3.1 R5 to adapt adequately the TOE security functional requirements of security in relation to including by the TSF a mechanism to ensure data integrity. These requirements differ from those specified in FAU_STG.1 as it specifies that the TSF must prevent or detect data alterations, leaving such operations out of scope in FAU_STG.5.

Component levelling

FAU_STG.5 Audit log signing event, incorporate a computation value to enable the detection of integrity of audit data.

Management: FAU_STG.5

There are no management activities foreseen.

Audit: FAU_STG.5

Minimal: compute value shall be included in the audit log.

FAU_STG.5 Audit log signing event

Hierarchical to:

No other components.

Dependencies:

FAU_GEN.1 Audit data generation

FCS_COP.1 Cryptographic operation

FAU_STG.5.1 The TSF must compute a value through **[assignment*: cryptographic operation*]** that is added to the audit data so that its integrity can be verified.

5.2 Class FKI: Security Key Infrastructure

The FKI class is defined as there is no class in Part 2: Security functional components of Common Criteria v3.1 R5 that defines requirements on specific assets of CA components that require specifications on their protection, such as the generation of X509 Certificates and CRLs as well such as the protection of specific data in its export.

5.2.1 Security Certificate X509 (FKI_CER)

Family Behaviour

The functions in this section address the issuance of public key certificates. X.509 public key certificates issued by the TSF must be compliant with the X.509 standard. Any fields or extensions to be included in an X.509 certificate will either be created by the TOE according to the rules of the X.509 standard or validated by the TSF to ensure compliance.

The data entered in each field and extension to be included in a certificate must be approved. Generally, a certificate field or extension value may be approved in one of four ways:

1) The data may be approved manually by an authorized user

2) The value for a field or extension may be automatically generated by the TSF.

3) The value for a field or extension may be taken from the certificate profile.

Rationale:

Its definition is justified since there is no component in CC Part 2 that can define the requirements that a Certification Authority (CA) must meet to issue X509 certificates and how the TSF must protect its public keys.

Component levelling

Management: FKI_CER.1, FKI_CER.2

There are no management activities foreseen.

Audit: FKI_CER.1

Minimal: all certificate requests shall be included in the audit log.

Audit: FKI_CER.2

There are no auditable events foreseen.

FKI_CER.1 – Certificate X509 Generation

Hierarchical to:

No other components.

Dependencies:

[FCS_COP.1 Cryptographic operation

or

FCS_COP.2 Delegated Cryptographic operation]

FKI_CER.1.1 The TSF shall only generate X509 certificates whose format complies with **[assignment: *standard*]**.

FKI_CER.1.2 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FKI_CER.1.3 The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FKI_CER.1.4 If the TSF generates X.509 public key certificates, it will only generate certificates that at least meet the following requirements:

a) The version field shall contain the integer 0, 1, or 2.
b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2.
c) If the certificate contains extensions, then the version field shall contain the integer 2.
d) The serialNumber shall be unique with respect to the issuing Certification Authority.
e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension.
h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS approved or recommended algorithm.

FKI_CER.2 Stored public key integrity

These security requirements are designed to detect the modification of public keys stored by the TSF.

Hierarchical to:

No other components.

Dependencies:

[FCS_COP.1 Cryptographic operation

or

FCS_COP.2 Delegated Cryptographic operation]

FKI_CER.2.1 The public keys will be protected by TSF against modifications invoking a specified cryptographic algorithm before being sent for storage **[selection:** digital signatures, keyed hashes, authentication codes**].**

5.2.2 Security Certificate Revocation List (FKI_CRL)

Family Behaviour

This family defines the requirements for the issuance of certificate revocation lists (CRLs).

Certificate revocation lists (CRLs) issued by the TSF shall be compliant with the X.509 standard. Any fields or extensions to be included in a CRL shall be created by the TSF according to the X.509 standard.

Rationale:

Its definition is justified since there is no component in CC Part 2 that can define the requirements that a Certification Authority (CA) must meet to issue X509 CRLs according to RFC5280.

Component levelling

FKI_CRL - Security Certificate Revocation List	1

Management: FKI_CRL.1

There are no management activities foreseen.

Audit: FKI_CRL.1

Minimal: all requests to change the status of a certificate must be registered in the audit log.

FKI_CRL.1 - Certificate revocation list generation

Hierarchical to:

No other components.

Dependencies:

[FCS_COP.1 Cryptographic operation

or

FCS_COP.2 Delegated Cryptographic operation]

FKI_CRL.1.1 A TSF that issues CRLs shall verify that any issued CRL contain at least the following elements:

a) If the version field is present, then it shall contain a 1.
b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
c) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
d) The signature and signatureAlgorithm fields shall contain the OID for a FIPS-approved digital signature algorithm.
e) The thisUpdate field shall indicate the issue date of the CRL.
f) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

5.2.3 Security Export Data (FKI_EXP)

Family Behaviour

This family defines the requirements for the exportation data from TSF to certificate status and user keys.

Rationale:

Its definition is justified since there is no component in CC Part 2 that can define the requirements that a Certification Authority (CA) must meet to export X509 CRLs and private keys of the users. The CC Part 2 defines the export of all user data but does not cover the need to be able to export a part of this user data and that this data must be in a format that protects its confidentiality or integrity.

Component levelling

Management: FKI_EXP.1, FKI_EXP.2

There are no management activities foreseen.

Audit: FKI_EXP.1, FKI_EXP.2

There are no auditable events foreseen.

FKI_EXP.1 - Certificate status export

The TSF must be capable of exporting certificate status information. The information on the status of the certificates will be exported in a format that meets a standard.

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FKI_EXP.1.1 Certificate status information shall be exported from the TSF in format complies with **[*assignment: standard*]**.

FKI_EXP.2 - User private key export protected

Keys may be exported from TSF for a variety of reasons, including key backup, replication, and transmission of user private keys generated in the TSF. These security requirements are designed for securing these exportations.

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FKI_EXP.2.1 User private key shall be exported from the TSF in format complies with **[*assignment: protected format*]**.

5.3 Cryptographic operation

We extend the class CLASS FCS: CRYPTOGRAPHIC SUPPORT defined in Part 2: Security functional components of Common Criteria v3.1 R5 to adapt adequately the TOE security functional requirements of security in relation to cryptographic operations used by the TOE.

Rationale:

The class extension of the class FCS: Cryptographic Support is justified since there is no component that establishes the cryptographic operations that are invoked by the TSF and which are made in its implementation by an external device. In this way, Cryptographic operation (FCS_COP) family expands with FCS_COP.2 a new level that establishes the delegation of cryptographic operations on an external device.

Component levelling

FCS_COP.2 Delegated Cryptographic operation, requires a cryptographic operation to be performed into an external device.

Management: FCS_COP.2

There are no management activities foreseen.

Audit: FCS_COP.2

There are no auditable events foreseen

FCS_COP.2 **Delegated cryptographic operation**

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.2.1 The TSF shall invoke an external device to perform **[assignment:** *cryptographic operations*]

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.
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
c) [***assignment:*** *The events listed in Table below*].

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, 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:*** *the information specified in the Additional Details column in Table below*]

NOTE: Additionally, the audit shall not include plaintext private or secret keys or other critical security parameters.

FUNCTION	EVENT	DETAIL
Audit	INIT_LOG_INTEGRITY	LogIntegrity Audit System startup
	END_LOG_INTEGRITY	LogIntegrity Audit System shutdown
Access Control	ACCESS_CONTROL	Authorization check to resource of authenticated entity
	ADMINWEB_ADMINISTRATORLOGGEDIN	An authorized user logs in to SIA CA's Administrative Web GUI
CA Management	CA_CREATION	Creation of a Certificate Authority
	CA_DELETION	Removal of a Certificate Authority
	CA_EDITING	Modification of a Certificate Authority

	CA_KEYACTIVATE	Certificate Authority starts using a different key pair
	CA_SERVICEACTIVATE	Certificate Authority state change to start serving requests. Unrelated to CA private key availability
	CA_SERVICEDEACTIVATE	Certificate Authority state change to stop serving requests. Unrelated to CA private key availability
	CA_RENEWED	Renewal of a Certificate Authority's certificate, optionally using a different key pair.
	CA_REVOKED	Revocation of a Certificate Authority and all certificates issued by it.
	CA_USERAUTH	End entity authenticates using enrollment code
	CA_USERAUTH	End entity authenticates using enrollment code
Certificate Management	CERT_STORED	Persistence of a certificate to the database
	CERT_REVOKED	Change of a certificate's status to revoked or active
	CERT_REQUEST	A request for certificate issuance from a Certificate Authority is submitted
	CERT_CREATION	Issuance of a certificate by a Certificate Authority
Certificate Profile Management	CERTPROFILE_CREATION	Creation of a certificate profile
	CERTPROFILE_DELETION	Removal of a certificate profile
	CERTPROFILE_RENAMING	Name change of a certificate profile
	CERTPROFILE_EDITING	Modification of a certificate profile

CRL Management	CRL_STORED	Persistence of a Certificate Revocation List to the database
	CRL_CREATION	Issuance of a Certificate Revocation List by a Certificate Authority
CryptoToken Management	CRYPTOTOKEN_CREATE	Creation of a Crypto Token
	CRYPTOTOKEN_EDIT	Modification of a Crypto Token
	CRYPTOTOKEN_DELETION	Removal of a Crypto Token
	CRYPTOTOKEN_ACTIVATION	Activation of a Crypto Token, making the key material available for use by the TOE
	CRYPTOTOKEN_DEACTIVATION	Deactivation of a Crypto Token, making the key material unavailable for use by the TOE
	CRYPTOTOKEN_DELETE_ENTRY	Removal of a key pair from the Crypto Token key material or key pair place-holder from the Crypto Token object
	CRYPTOTOKEN_GEN_KEYPAIR	Generation of a new key pair in the Crypto Token
Validators Management	VALIDATOR_CHANGE	Modification of an existing validator
	VALIDATOR_CREATION	Creation of a new validator
	VALIDATOR_REMOVAL	Removal of an existing validator
	VALIDATOR_RENAME	Name change of an existing validator
Role Management	ROLE_CREATION	Creation of an administrative role
	ROLE_DELETION	Removal of an administrative role
	ROLE_RENAMING	Name change of an administrative role
	ROLE_ACCESS_RULE_CHANGE	Modifications of existing access rules in a role
	ROLE_ACCESS_USER_ADDITION	New authorized user added to role

	ROLE_ACCESS_USER_DELETION	Removal of existing authorized user from role
Approval Management	APPROVAL_ADD	Action that requires approval by one or more administrators is requested
	APPROVAL_APPROVE	Action that requires approval was approved by one of the required authorized user(s)
	APPROVAL_REJECT	Action that requires approval was rejected by one of the required authorized user(s)
	APPROVAL_PROFILE_ADD	Adding an approval profile
	APPROVAL_PROFILE_EDIT	Editing an approval profile
	APPROVAL_PROFILE_REMOVE	Removing an approval profile
	APPROVAL_PROFILE_RENAME	Renaming an approval profile
Publisher Management	PUBLISHER_CHANGE	Modification of an existing publisher
	PUBLISHER_CREATION	Creation of a new publisher
	PUBLISHER_REMOVAL	Removal of an existing publisher
	PUBLISHER_RENAME	Name change of an existing publisher
	PUBLISHER_STORE_CERTIFICATE	Publishing of a certificate and/or related certificate meta data
RA Management	RA_ADDEEPROFILE	Creation of a new end entity profile
	RA_ADDENDENTITY	Creation of a new end entity
	RA_DELETEENDENTITY	Removal of an end entity
	RA_EDITEEPROFILE	Modification of an existing end entity profile
	RA_EDITENDENTITY	Modification of an existing end entity
	RA_REMOVEEEPROFILE	Removal of an existing end entity profile

	RA_RENAMEEEPROFILE	Name change of an existing end entity profile
	RA_REVOKEDENDENTITY	Change status of an existing end entity and all the end entity's certificates to revoked

Table 7: Auditable Events and Audit Data

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.
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.

6.1.1.3 FAU_STG.5 Audit log signing event

Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation
FCS_COP.1 Cryptographic operation

FAU_STG.5.1 The TSF must compute a value through **[assignment***: compute the HMAC value***]** that is added to the audit data so that its integrity can be verified.

6.1.2 Roles

The ability to perform many of the functions specified in this ST will be allocated to distinct roles to maintain the security of the TOE.

6.1.2.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[*assignment*:** *Super Administrator Role, CA Administrators, RA Administrators, Auditor, Supervisors and Custom Roles***].**

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

NOTE: No specified TOE role, including the Auditor role, will be able to access the audit data generated by FAU_GEN through a TOE interface, only an auditor or administration user from the operating environment will be able to perform audit data query and analysis operations by accessing through the operating environment.

6.1.2.2 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to **[*selection: modify the behavior of*]** the functions **[*assignment: CryptoToken Management, CA Management, Certificate Profile Management, End Entity Management, End Entity Profile Management, TOE Configuration*]** to **[*assignment: listed to the authorized roles as specified in Table below*]**.

SECTION/FUNCTION	AUTHORIZED ROLE
CryptoToken Management	The capability to create, delete and modify CryptoTokens and your associated keys for Certification Authorities shall be restricted to Super Administrators and Custom Role with the necessary assigned permissions.
CA Management	The capability to create Certification Authorities shall be restricted to Super Administrators Role.
	The capability to modify and delete Certification Authorities shall be restricted to Super Administrators, CA Administrators and Custom Role with the necessary assigned permissions. Note that CA Administrators Role are not authorized to generate new keys, only renew using existing ones.
	The capability to modify the CRL configuration shall be restricted to Super Administrators, CA Administrators and Custom Role with the necessary assigned permissions.
Certificate Profile Management	The capability to create, modify and delete certificate profile shall be restricted to Super Administrators, CA Administrators and Custom Role with the necessary assigned permissions.
End Entity Management	The capability to create, modify, revoke and delete End Entities shall be restricted to Super Administrators, CA Administrators, RA Administrators and Custom Role with the necessary assigned permissions.
End Entity Profile Management	The capability to create, modify and delete End Entity profiles shall be restricted to Super Administrators, CA Administrators and Custom Role with the necessary assigned permissions.
TOE Configuration	The capability to configure any TSF functionality shall be restricted to Super Administrators and Custom Role with the necessary assigned permissions.

Table 8: Authorized Roles for Management of Security Functions Behavior

6.1.3 Access Control

6.1.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the **[*assignment: TOE Access Control Policy specified in section 8*]** on **[*assignment: Subjects: all users of the TOE; Objects: any object; Operations: any operation except HealthCheck request for TOE status monitoring purposes*]**.

6.1.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the **[*assignment: TOE Access Control Policy specified in section 8*]** to objects based on the following: **[*assignment*: *the identity of the subject and the set of roles that the subject is authorized to assume according to the indicated policy*].**

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:**

- ***Access of subjects <authorized users>***
    - ***That the authentication certificate sent in the request exists registered in the system and is associated with an End Entity.***
    - ***That after passing the user authentication process, the user has an associated role where sufficient execution permissions are established for the operations requested through the functionalities available in the TOE services.***

].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[*assignment: no additional rules*].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
[*assignment: no additional rules*].

6.1.4 Identification and Authentication

Identification and authentication include recognizing an entity (e.g., user, device, or system) and verifying the identity of that entity.

6.1.4.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[*assignment: status request over HealthCheck operation*]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

6.1.4.2 FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow **[*assignment: status request over HealthCheck operation*]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

6.1.4.3 FIA_USB.1 User-subject binding

Hierarchical to: No other components.
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: the set of roles of the user*]**.

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: the object that will represent the user's identification will be assigned the role*]**.

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*]**.

6.1.4.4 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***assignment***: *End Entity, Role, Authentication certificate*].

6.1.5 Management of security attributes

6.1.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[*assignment*: *TOE Access Control Policy specified in section 8*]** to restrict the ability to **[*selection*: *change_default, query, modify, delete*, [*assignment*: *none*]]** the security attributes **[*assignment*: *roles, end entities and authentication certificates*]** to **[*assignment*: *authorized users*]**.

NOTE: Certificates cannot be modified or deleted, their status can simply be changed in the system, but they will remain stored for their corresponding revocation control.

6.1.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[*assignment*: *TOE Access Control Policy specified in section 8*]** to provide **[*selection, choose one of*: *restrictive*]** default values for security attributes that are used to enforce the SFP.

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

6.1.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- *CryptoToken Management*
- *End Entity Management*
- *End Entity Profile Management*
- *CA Management*
    - *CRL Configuration: Allow the authorised users to specify the set of acceptable values for the following fields and extensions:*
        - *issuer*
        - *issuerAltName*
        - *nextUpdate*
        - specify the acceptable set of CRL and CRL entry extensions
- *Certificate Profile Management*
    - *Allow the authorised users to specify the set of acceptable values for the following fields and extensions:*
        - *the key owner's identifier.*
        - *the algorithm identifier for the subject's public/private key pair.*
        - *the identifier of the certificate issuer.*
        - *the length of time for which the certificate is valid.*
        - *keyUsage*
        - *basicConstraints*
        - *certificatePolicies*
        - *specify the acceptable set of certificate extensions.*
- *TOE Configuration].*

6.1.6 Remote Data Entry and Export

6.1.6.1 FCO_NRO.1 Selective proof of origin

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted **[*assignment*: *X509 Certificate*]** at the request of the **[*selection: originator*].**

FCO_NRO.1.2 The TSF shall be able to relate the **[*assignment: End Entity*]** of the originator of the information, and the **[*assignment*: *X509 Certificate*]** of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to **[*selection: originator*]** given **[*assignment*: *match with authorized user X509 certificate*]**.

6.1.6.2 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the **[*assignment*: *TOE Access Control Policy specified in section 8*]** to **[*selection*: *transmit, receive*]** user data in a manner protected from unauthorised disclosure.

6.1.7 Cryptographic operations

6.1.7.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**assignment:** *compute HMAC value*] in accordance with a specified cryptographic algorithm [**assignment**: *MAC with SHA-256 hashing*] and cryptographic key sizes [**assignment**: *SHA-256*] that meet the following: [**assignment**: *HMAC-SHA-256*].

6.1.7.2 FCS_COP.2 Delegated Cryptographic operation

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_COP.2.1 The TSF shall invoke an external device to perform **[assignment:** *digital signature*]

6.1.8 FKI Operation

6.1.8.1 FKI_CER.1 Certificate X509 Generation

Hierarchical to: No other components.
Dependencies: [FCS_COP.1 Cryptographic operation
or
FCS_COP.2 Delegated Cryptographic operation]

FKI_CER.1.1 The TSF shall only generate certificates whose format complies with **[*assignment: RFC 5280*]**.

FKI_CER.1.2 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FKI_CER.1.3 The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FKI_CER.1.4 If the TSF generates X.509 public key certificates, it will only generate certificates that at least meet the following requirements:

a) The version field shall contain the integer 0, 1, or 2.
b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2.
c) If the certificate contains extensions then the version field shall contain the integer 2.
d) The serialNumber shall be unique with respect to the issuing Certification Authority.
e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension.
h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS approved or recommended algorithm.

6.1.8.2 FKI_CER.2 Stored public key integrity

Hierarchical to: No other components.
Dependencies: [FCS_COP.1 Cryptographic operation
or
FCS_COP.2 Delegated Cryptographic operation]

FKI_CER.2.1 The public keys will be protected by TSF against modifications invoking a specified cryptographic algorithm before being sent for storage **[selection:** digital signatures**]**.

6.1.8.3 FKI_CRL.1 Certificate revocation list generation

Hierarchical to: No other components.
Dependencies: [FCS_COP.1 Cryptographic operation
or
FCS_COP.2 Delegated Cryptographic operation]

FKI_CRL.1.1 A TSF that issues CRLs shall verify that any issued CRL contain at least the following elements:

a) If the version field is present, then it shall contain a 1.
b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
c) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
d) The signature and signatureAlgorithm fields shall contain the OID for a FIPS-approved digital signature algorithm.
e) The thisUpdate field shall indicate the issue date of the CRL.
f) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

6.1.8.4 FKI_EXP.2 User private key export protected

Hierarchical to: No other components.
Dependencies: No dependencies.

FKI_EXP.2.1 User private key shall be exported from the TSF in format complies with **[assignment:** *PKCS#12, JKS*]**.**

NOTE: The export of the keystore through the TOE webservices will be carried out by returning the keystore but encoded in Base64.

6.1.8.5 FKI_EXP.1 Certificate status export

Hierarchical to: No other components.
Dependencies: No dependencies.

FKI_EXP.1.1 Certificate status information shall be exported from the TSF in format complies with **[assignment:** *X.509 standard RFC 5280 for CRLs*]**.**

NOTE: The export of the CRLs through the TOE webservices will be carried out by returning the CRL in X509 standard format but encoded in Base64.

6.2 Requirement Dependency Rationale

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole. Internal consistency is demonstrated in an analysis of dependencies. Mutual support is shown through consideration of the interactions between and among the SFRs.

6.2.1 Rationale that Dependencies Are Satisfied

The selected security requirements include related dependencies, both direct and indirect. The indirect dependencies are those required by the direct dependencies. All these dependencies must be met, or their exclusion justified.

6.2.1.1 Security Functional Requirements Dependencies

The following table provides a summary of the security functional requirements dependency analysis.

COMPONENT	DEPENDENCIES	WHICH IS:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included in the IT Environment
FAU_GEN.2 User identity association	GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included

FAU_STG.5 Audit log signing event	FAU_GEN.1 Audit data generation FCS_COP.1 Cryptographic operation	Included
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Included
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FIA_ATD.1 User attribute definition	None	
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included Included
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	FMT_MOF.1 Management of security functions behavior FMT_SMR.1 Security roles	Included Included

FCO_NRO.1 Selective proof of origin	FIA_UID.1 Timing of identification	Included
FDP_UCT.1 Basic data exchange confidentiality	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset informationflow control] FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	FDP_ACC.1 Included FTP_TRP.1 Included in the IT Environment
FCS_COP.1 Cryptographic operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Not Included
FCS_COP.2 Delegated Cryptographic operation	None	
FKI_CER.1 Certificate X509 generation	FCS_COP.1 Cryptographic operation or FCS_COP.2 Delegated Cryptographic operation	Included
FKI_CER.2 Stored public key integrity	FCS_COP.1 Cryptographic operation or FCS_COP.2 Delegated Cryptographic operation	Included
FKI_CRL.1 Certificate revocation list generation	FCS_COP.1 Cryptographic operation or FCS_COP.2 Delegated Cryptographic operation	Included
FKI_EXP.1 Certificate status export	None	

FKI_EXP.2 User private key export	None	

Table 9: Summary of Security Functional Requirements Dependencies

6.2.1.1.1 Justification of Unsupported Dependencies Regarding FTP_ITC.1 or FTP_TRP.1

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter- TSF trusted channel or FTP_TRP.1 Trusted path that is unmet. The secure channel between third parties and the TOE is established as a requirement of the operating environment **OE.Trusted Path** so that TSFs can only be accessed through channels that ensure data confidentiality and integrity.

6.2.1.1.2 Justification of Unsupported Dependencies Regarding FPT_STM.1

The following components depend on FPT_STM.1 Reliable time stamps:

- FAU_GEN.1 Audit data generation

The FAU_GEN.1 requirement does not comply with the FPT_STM.1 Reliable time stamps dependency since it is not a security functionality of the TOE to ensure the date and time reflected in the audit files. The TOE collects the date and time of the system that can be configured so that it can be synchronized with time servers using the ntp protocol via **OE.Time stamps.**

6.2.1.1.3 Justification of Unsupported Dependencies Regarding FCS_COP.1 Cryptographic operation

The following components depend on *FCS_COP.1 compute HMAC for audit*:

- [FDP_ITC.1 Import of user data without security attributes,
  or FDP_ITC.2 Import of user data with security attributes,
  or FCS_CKM.1 Cryptographic key generation]
  FCS_CKM.4 Cryptographic key destruction

The *FCS_CKM.1 Cryptographic key generation* requirement does not comply with the *FCS_COP.1 compute HMAC for audit* dependency since the key is generated during the installation of the TOE by a process that is outside the scope of the TOE itself as stated in **OE.Security-relevant configuration management** and is protected against unauthorized access via **OE.Physical Protection.**

Likewise, *FCS_CKM.4 Cryptographic key destruction* is not fulfilled since the key cannot be destroyed because the key must remain available to validate the integrity of the data at any time.

6.3 Security Requirements Rationale

This section provides the rationale for necessity and sufficiency of security requirements, demonstrating that each of the security objectives is addressed by at least one security requirement and that every security functional requirement is directed toward solving at least one objective.

FUNCTIONAL REQUIREMENT	OBJECTIVE
FAU_GEN.1 Audit data generation	O.Individual accountability and audit records
FAU_GEN.2 User identity association	O.Individual accountability and audit records
FAU_STG.5 Audit log signing event	O.Protect stored audit records
FMT_SMR.1 Security roles	O.Limitation of administrative access O.Security roles
FMT_MOF.1 Management of security functions behavior	O.Configuration management
FDP_ACC.1 Subset access control	O.Limitation of administrative access
FDP_ACF.1 Security attribute based access control	O.Limitation of administrative access
FIA_UAU.1 Timing of authentication	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_USB.1 User-subject binding	O.Maintain user attributes
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FMT_MSA.1 Management of security attributes	O.Limitation of administrative access O.Maintain user attributes
FMT_MSA.3 Static attribute initialisation	O.Limitation of administrative access O.Maintain user attributes
FMT_SMF.1 Specification of Management Functions	O.Configuration management
FCO_NRO.1 Selective proof of origin	O.Non-repudiation,
FDP_UCT.1 Basic data exchange confidentiality	O.Data import/export

FCS_COP.1 Cryptographic operation	O.Protect stored audit records
FCS_COP.2 Delegated Cryptographic operation	O.Certificates
FKI_CER.1 Certificate X509 Generation	O.Certificates
FKI_CRL.1 Certificate revocation list generation	O.Certificates
FKI_EXP.1 Certificate status export	O.Certificates
FKI_EXP.2 User private key export	O.Data import/export
FKI_CER.2 Stored public key integrity	O.Certificates

Table 10: Security Functional Requirements Related to Security Objectives

6.3.1 Security Requirements Sufficiency

This section demonstrates the adequacy of the established security functional requirements to cover all the security objectives of the TOE.

- **O.Certificates:** The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.

  FKI_CER.1 Certificate X509 Generation, FKI_CER.2 Stored public key integrity, **FCS_COP.2 Delegated Cryptographic operation** and **FKI_CRL.1 Certificate revocation list generation** ensures that issued certificate and certificate revocation lists are valid and **FKI_EXP.1 Certificate status export** ensures that certificate status information is valid and protected.

- **O.Non-repudiation:** Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.

  By means of **FCO_NRO.1 Selective proof of origin** the system ensures that requests that do not come from a reliable source will not be accepted through proof of origin by means of client authentication using the electronic signature for this purpose and thus determine the origin of the request.

- **O.Data import/export:** Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

  By means of **FDP_UCT.1 Basic data exchange confidentiality** the requirement that data is protected when transmitted to the TOE is covered.
  FKI_EXP.2 User private key export protected covers the requirement that keys are protected when exported from the TOE.

- **O.Individual accountability and audit records:** Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.

  The analysis of the audit data will be carried out by auditors through the mechanisms that the operating environment establishes to access said data. The analysis and consultation of audit data is not part of the scope of the TOE.

  By means of **FIA_UID.1 Timing of identification** where the requirement of identifying the user before performing any security function is covered and by means of **FAU_GEN.1 Audit**

data generation, FAU_GEN.2 User identity association where the requirement of generating the audit traces where the entity responsible for the event is identified together with the date of performance is covered.

- **O.Limitation of administrative Access:** Design administrative functions so that authorized users do not automatically have access to user objects, except for necessary exceptions. Control access to the TOE by authorized users who operate the TOE.

  By means of **FDP_ACC.1 Subset access control, FDP_ACF.1 Security attribute based access control, FIA_UAU.1 Timing of authentication and FIA_UID.1 Timing of identification** an access and authentication control is established through which it is ensured that all users must be identified and authenticated before any operation is performed on the system.
  The roles to which the users must belong are specified in order to be able to carry out only the operations authorized by **FMT_SMR.1 Security roles** and the management of security attributes is established by **FMT_MSA.1 Management of security attributes and FMT_MSA.3 Static attribute initialization.**

- **O.Security roles:** Maintain security-relevant roles and the association of users with those roles.

  FMT_SMR.1 Security roles covers the requirement where the necessary roles are maintained and the association of those roles with the TOE users.

- **O.Protect stored audit records:** ensures that audit logs contain an HMAC value that enables detection of unauthorized modification or removal to provide traceability of user actions.

  With **FAU_STG.5 Audit log signing event and FCS_COP.1 Cryptographic operation** the cover the requirement to include the HMAC value into audit data.

- **O.Restrict actions before authentication:** Restrict the actions a user may perform before the TOE authenticates the identity of the user.

  FIA_UAU.1 Timing of authentication covers the requirement that before any security function can be performed, the user must first be authenticated.

- **O.Configuration Management:** Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.

  FMT_MOF.1 Management of security functions behavior, **FMT_SMF.1 Specification of Management Functions** covers the requirement that a configuration is established in the system that allows the issuance of certificates and crls and that only authorised personnel can modify this configuration.

- **O.Maintain user attributes:** Maintain a set of security attributes (which may include role membership. Access privileges, etc.) associated with individual users.

  FIA_USB.1 User-subject binding, FIA_ATD.1 User attribute definition, FMT_MSA.1 Management of security attributes and FMT_MSA.3 Static attribute initialization covers the requirement to maintain the individual security attributes by users as well as the default values assigned and that these can be managed by users with the appropriate privileges.

6.4 Security Assurance Requirements

The development and evaluation of the TOE will be carried out according to the guarantee level EAL 4 + ALC_FLR.1.

The requirements for this level of assurance, as specified in Common Criteria Part 3 v3.1 R5, are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.1: Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 11: Assurance Requirements

Predefined package EAL4 allows users to rely in the product since it is developed using high standard development practices.

The addition of ALC_FLR.1 provides assurance that flaws will be addressed and fixed.

7 TOE Summary Specifications

7.1 Access Control

Any access requires authentication through certificates in the communication channel established with the TOE and before performing any operation, the user requesting the operation is identified.

- FIA_UAU.1 Timing of authentication: authentication is required to perform any operation through the TOE interfaces that perform security functions.

- FIA_UID.1 Timing of identification: identification is required to perform any operation through the TOE interfaces that perform security functions.

- FIA_USB.1 User-subject binding: User security attributes are associated to the TOE user identity and authentication credentials, allowing a unique match.

- FIA_ATD.1 User attribute definition: Allows each user to maintain their individual security attributes such as their identifier, the role, or roles they belong to and their authentication certificate.

The TOE's resources are protected using access control lists, based on four key components:

- access rule – accept or decline access to a resource, can be recursive or not;
- resource – a resource to which access is controlled.
- user – an entity that have access rights to a resource;
- role – a role that a user is allowed to take on. Since access rules are defined on a role, so for a user to have access rights he must be assigned roles.

The TOE verifies in each operation that the user who invokes the operation has sufficient permissions to access the specified resource, otherwise the operation is rejected.

- FDP_ACC.1 Subset access control: Access control lists can be used to specify the acceptable subsets of security functions applicable to specified resources.

- FDP_ACF.1 Security attribute based access control: TOE users are assigned roles that are granted a set of access control rules on a set of resources.

- FMT_SMR.1 Security roles: It establishes the necessary roles to establish the correct access to the TOE security functions.

- FMT_MOF.1 Management of security functions behavior: The Access Control uses the defined Roles the evaluate whether the TOE user shall be granted access to the requested object or operation.

- FMT_MSA.1 Management of security attributes: Management of security attributes is established to determine access to resources and to be able to assign roles to users.

- FMT_MSA.3 Static attribute initialization: The default value is to restrict access to resources until an administrator manages it.

7.2 Key Management

The keys of the CAs will be stored in a cryptographic module and the TOE will invoke the cryptographic operations so that the electronic signatures made for the issuance of certificates by the CA are assured.

The public keys stored in the database will be saved in a certificate with X509 format complying with RFC 5280 signed by the issuing CA.

- FKI_CER.1 Certificate X509 generation: The TSF generates certificates according to the X.509 and RFC 5280 standard.

- FCS_COP.2 Delegated Cryptographic operation: The TSF invoke the digital signature to issue the X509 certificate using the private key inside the cryptographic module.

- FKI_CER.2 Stored public key integrity: The integrity and authenticity of public keys stored by the TOE is protected by the usage of a digital signature, the public key will always be stored in a signed X509 certificate format to protect its integrity.

7.3 Management of the issuance of certificates and CRLs

The TOE uses profiles and configuration that are generated by administrator users to issue certificates and CRLs, these certificates and CRLs are generated based on standards.

To carry out these operations, the TOE has functions through its interfaces that manage the complete life cycle of a certificate, in this way the issuance, renewal, revocation, etc. of the certificates can be requested. The certificates will be issued based on profiles previously configured by administrator users according to the type of certificate, therefore defining important characteristics such as extensions associated with the certificate.

Likewise, the TOE will issue CRLs based on the RFC 5280 standard, where you can check the revocation status of a certificate.

- FMT_SMF.1 Specification of Management Functions: The profiles establish key characteristics of the certificate such as algorithms, key sizes, extensions, keyusage, etc.

  It also defines the characteristics of CRL issues.

- FKI_CER.1 Certificate X509 generation: The TSF generates certificates according to the X.509 and RFC 5280 standard.

- FCS_COP.2 Delegated Cryptographic operation: The TSF invoke the digital signature to issue the X509 certificate and CRLs using the private key inside the cryptographic module.

- FKI_CRL.1 Certificate revocation list generation: The TSF generates CRLs according to the X.509 and RFC 5280 standards.

7.4 Data transmission security

Regarding data entry and exit, the TOE is capable of handling and processing:

- FCO_NRO.1 Selective proof of origin: Digital signatures are used as a basis for ensuring proof of origin, given the compliance with X.509 v3.

- FDP_UCT.1 Basic data exchange confidentiality: In all accesses to the TOE through its interfaces where sensitive data is accessed, an access control policy is applied that determines the level of privileges of the authorized user, in this way the confidentiality of the data is protected by not being able to access them to unauthorized users.

- FKI_EXP.1 Certificate status export: Certificate status information is provided by the TSF through CRLs compliant with X.509 RFC 5280 standard.

- FKI_EXP.2 User private key export: User private keys can only be exported from the TOE in PKCS#12 format or JKS format.

7.5 Audit Data

Audit includes a chronological recording of events that occur in a system. The objective is to track what occurs to enable the reconstruction and examination of a sequence of events and/or changes in an event. This is useful in ensuring that the system is operated securely and in providing evidence when a suspected or actual security compromise has occurred. Audit also provides for reconstructing a specific state of a system. The objective in a PKI system is to enable an appropriate authority to determine whether a signature should have been accepted as valid.

The audit will be used to reconstruct important events that were performed by the TSF, such as issuance of a CA certificate, and the user or event (e.g., a signed certificate request) that caused them. The audit will be used to arbitrate future disputes by establishing the validity of a signature at a particular time. The audit log records the security-relevant events that were performed by the TSF and the users or events (e.g., a signed certificate request) that caused them. This subsection specifies the security requirements for maintaining and protecting the integrity of the audit logs.

The TSF generates the following audit log type:

• *audit trail*, the TSF generates audit logs with the most relevant security events and includes an HMAC value to enable the validation of its integrity.

Each log entry reflects the event data that occurred with the following information:

- Date/time; Time of operation.
- User: User that originated the event.
- Service Type: Type of service that generated the operation.
- Module: Module that generated the operation.
- Event Type: Description of the operation.
- Other details. Additional information of the operation.
- Result: Operation result (OK or error).

The audit trails are stored locally in files on the machine where the TOE resides, in this way a user with privileges will be able to access them for export.

The TOE ensures at all times that these logs will not write any sensitive information that must be protected confidentially, such as passwords, keys, etc.

The TOE ensures that all events are recorded, so that if for any reason, for example insufficient space to generate the audit log, the operation will be rejected to prevent operations from being carried out without being recorded.

The precision of the date and time recorded for each operation in the log is guaranteed through the operating environment synchronizing with a reliable source of time.

- FAU_GEN.1 Audit data generation: The audit logs are generated immediately after the operation and are stored in the file that resides on the same machine as the TOE, the operation will not be considered performed if it is not correctly registered in the log.

- FAU_GEN.2 User identity association: Audit logs include information about the user invoking the operation.

- FAU_STG.5 Audit log signing event and FCS_COP.1 Cryptographic operation, Audit logs includes an HMAC value to enable the validation of its integrity.

8 TOE Access Control Policy

This appendix describes the characteristics of the access control policy that the TOE will enforce and manage.

The system will grant subjects access to objects and operations made over it based upon:

a) The identity of the subject that requested the access through your authentication certificate.
b) The role(s) associated to that subject.
c) The details of the access request that will indicate the resource to be accessed

These subjects are defined in the system with the name of End Entity, and although there may be a multitude of End Entities created in the system, only those with the previously defined security attributes are defined as authorized users.

Authorized users are defined as all those End Entities who are assigned the three attributes previously indicated.

Authorized user identification includes individuals assigned to one or more roles with different access authorizations.

Access to objects is defined by the simple access types used on access rules:

- Allow
- Deny
- Inherit

Access rules can be organized hierarchically and Allow and Deny access types can be applied recursively indicating the inherited value.

The default access decision for an Inherit access rule is to deny access, unless there is a hierarchically superior access rule with value Allow that applies recursively.

It is determined that only authorized users have access to the TOE interfaces and that this access control policy will be always applied for their authentication and authorization.

The TOE supports default role designed to cover most use cases and be easily extendable:

Predefined Role:

- **Super Administrator Role**
  - Has overall access to TOE
- **CA Administrators**
  - CA Management Functions
- **RA Administrators**
  - RA Management Functions
- **Supervisors**
  - Supervision Functions
- **Auditor**
  - Audit Functions

Additionally, the TOE supports the definition of custom roles where different functionalities and privileges can be established from a template called Custom.

- **Custom**
  - You can build custom roles to limit access to the level you want to set.

9 Normative References

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev. 5, April 2017.

- Part 1: Introduction and general model.
- Part 2: Security functional components.
- Part 3: Security assurance components.

[2] Common Methodology for Information Technology Security Evaluation CEM, Version 3.1, Rev. 5, April 2017.

[3] ISO/IEC 15408 (Common Criteria) Information technology -- Security techniques -- Evaluation criteria for IT security.

[4] ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules.

[5] FIPS PUB 140-2 Security Requirements for Cryptographic Modules.

[6] ETSI/TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

10 Acronyms and Terminology

API: Application Programming Interface.

DDBB: Data Base.

CA: Certification Authority

CC: Common Criteria.

CRL: Certification Revocation List

CSR: Certificate Signing Request.

EAL: Evaluation Assurance Level.

HSM: Hardware Security Module.

HTTP: Hypertext Transfer Protocol.

IT: Information Technology.

PKI: Public Key Infrastructure.

PKCS: Public-Key Cryptography Standards.

PKCS#10: Certification application standard. Format of messages sent to a Certification Authority to request certification of a public key.

PKCS#11: Cryptographic device interface. Defines a generic API for access to cryptographic devices.

PP: Protection Profile.

RA: Registry Authority.

SF: Security Function.

SFP: Security Function Policy.

SFR: Security Functional Requirements.

SSL: Secure Sockets Layer.

ST: Security Target.

TLS: Transport Layer Security.

TOE: Target of Evaluation.

TSF: TOE Security Functions.

An Indra company

SIA

Av. de Europa, 2
28922 Alcorcón, Madrid
T +34 91 307 79 97

sia.es