SECURITY TARGET FOR SERVER SIGNING APPLICATION

Title:	Security target for Server Signing Application
Document type:	Definición de requisitos
File name:	Ancert server signing application security target v1.10.docx
Version:	1.10
Status:	Aprobado
Data classification:	Confidencial
Date:	16/04/2019
Author:	Pau del Canto

Revision / Approval		
Reviewed by:	Enric Hernández	Date: 16/04/2019
Approved by:	Enric Hernández	Date: 16/04/2019

Change history			
Version	**Date**	**Action**	**Pages**
1.0	30/08/2016	Document creation.	
1.0.1	11/10/2016	OR003-M0 resolution.	
1.0.2	16/11/2016	OR003-M1, OR008-M0 and comments resolution	
1.0.3	24/11/2016	Physical scope updated.	
1.0.4	12/01/2017	User and roles definition review (OR018-M0). Some software versions in section 2.3.4 detailed (OR014-M0). Added three new security objectives for the environment in section 5.2. (OR015-M0) SFR list review and correction (OR017-M0).	
1.0.5	26/01/2017	Added [SOGCRYPT] as reference guide for data encryption algorithms selection. Fix Java execution environment version. Remove Signer role from TOE summary specification.	
1.0.6	28/03/2017	OR022-M0 resolution.	
1.1	05/04/2017	New version numbering scheme. Update references to other CC documents. RDBMS versions refinement.	

1.2	14/12/2017	Update references to other CC documents.	
1.3	14/12/2017	HSM certification requirements changed from FIPS 140-2 L3 to Common Criteria EAL4+AVA_VAN.5. TOE's evaluation assurance level augmented to EAL4+AVA_VAN.5, ALC_FLR.2 Minor update in the TOE functionality regarding the audit integrity	
1.4	22/05/2018	Minor update due to inconsistencies	
1.5	30/05/2018	Minor updates due to inconsistencies and modifications after TSP audit	
1.6	25/07/2018	Periodic integrity checks added.	
1.7	24/09/2018	Minor assumption changes regarding database access and other minor changes.	
1.8	25/02/2019	OR007-M0 resolution.	
1.9	01/03/2019	Changes on document classification and approval	
1.10	16/04/2019	Changes on document because of laboratory request	

1. Table of contents

2. Introduction

2.1. Identification

Document identifier:	SECURITY TARGET FOR SERVER SIGNING APPLICATION
Document version:	1.10
TOE name:	ANCERT Server Signing Application
TOE version:	1.1.8
Created by:	ANCERT
Publication date:	16/04/2019

2.2. Product general description

ANCERT Server Signing Application (ANCERT SSA) is part of a Trustworthy System for Server Signing (TW4S) solution that managed by a Trusted Service Provided and operated in a secured environment is designed to work as Qualified Signature Creation Device as defined in EU 910/2014 Annex II.

2.3. TOE Overview

2.3.1 TOE Type

The TOE corresponds to a software component running on an operating system that provides remote signature generation services to Signer.

2.3.2 TOE Usage

The TOE security functionalities are accessed through three REST interfaces only accessible through secure channels:

- Administrative interface.
- RA interface.
- Signer interface.

All three interfaces require users to by identified and authenticated prior to access and execute any operation over the objects managed by the TOE. Authorization decisions are based on user roles and object attributes.

The RA and Signer interfaces can be invoked remotely. The Administrative interface is not accessible remotely enforcing that the management operations are performed from the same server and in the same physically secured environment where the TOE is installed.

RA applications accessing the RA interface are authenticated using TLS certificate based client authentication. The TOE security functionalities accessible in this interface are Signer's key pair (SCD/SVD) creation, and SCD activation / deactivation.

Cloud Keys Store Provider (CloudKSP) is the name given to the applications authorized to access the Signer interface. The signer interface also requires TLS certificate based client authentication. The TOE security functionalities accessible in this interface are Signer's signature requests and Signer's requests for changing the PIN used as one authentication factor to access the Signer's SCD.

The CloudKSP also manages the communications between the SCA and the TOE. When the Signers' using an SCA requests a digital signature over a document to be done with a SCD managed by the SSA, the CloudKSP requires the Signers' to activate the SCD with a message to the SSA. The Signers' sends the SAD in response to the CloudKSP request using his SAA, and finally the CloudKSP forwards the SAD to the TOE.

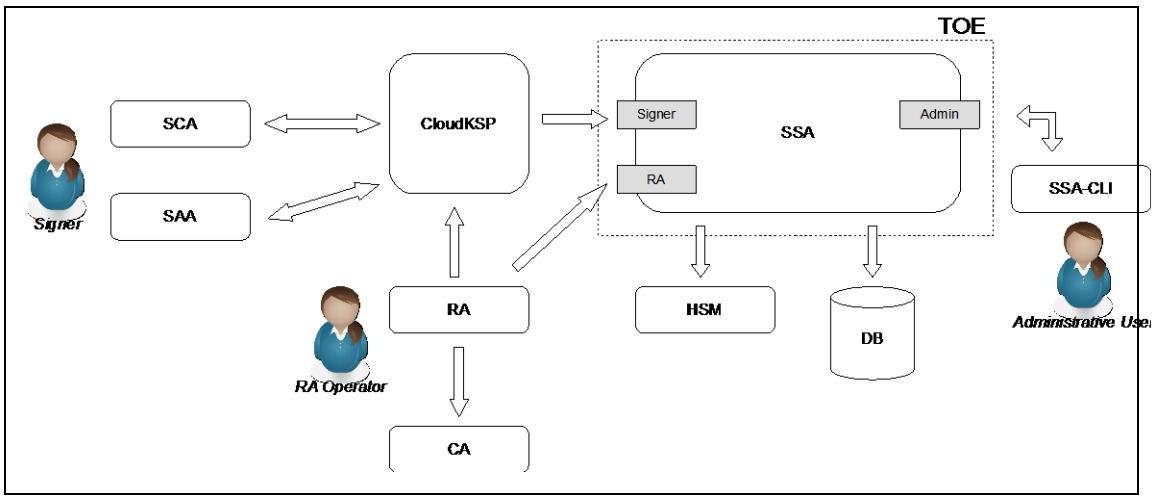


Figure 1 – TW4S solution including the SSA (TOE) with its interfaces and users

2.3.3 Major security features of the TOE

The TOE is a software component that provides services for the generation of remote signature in a manner that:

- It is able to receive and process Data to Be Signed Requests (DTBS/R) from external Signer or Signature Creation Application (requesters), protecting the integrity of the requests when managed by the TOE.
- The integrity of the signed document produced by the TOE is protected when created and managed by the TOE and during transfer from the TOE to an external entity.
- Any external entity can verify the authentication of the signed document produced by the TOE.
- The TOE services (TOE initialization, start of TOE operation, stop of TOE operation, TOE configuration, generation of Signer's key pair (SCD and SVD), Signer's public key (SVD) export for certificate request, certificate import, signature export, signer bundle, Signer SAP information and internal audit) are only used in an authorized way.
- Manages (generation, backup, usage and destruction) SCD and SVD of the Signer using an external HSM, and authentication information of the Signer provided by SCA or external trusted source and produce CSR in order to be delivered to CA.

- Links a Signer to SAP/SAD with SCD and SVD and DTBS/R in order to guaranty that the Signer has sole control over his SCD.
- Two independent authenticator factors are combined in the SAD/SAP in order to gain access to Signer's SCD.
- It is able to produce an audit trail where all the security events and all the Signer's interactions with his SCD are logged.
- Protects the integrity and authenticity of the TOE configuration data, signer bundles and audit trail.

2.3.4 Non TOE Hardware and Software

The TOE by itself is not able to ensure the complete security of the signature generation process and shall be operated in an environment that meets the requirement described in this section.

Hardware and other software components (e.g. operating system, drivers, Hardware Security Module (HSM), and other software applications) that might be needed by the TOE to provide its services are considered part of the TOE operational environment.

The TOE needs, at least, the following hardware/software/firmware to operate:

- Server running the main system:
  - 2 CPU x64 @ 2.0 GHz, 4GB RAM, 40 GB HD
- Operating System:
  - Red Hat EL 6 x64
- Server software:
  - Java Runtime Environment: Oracle JDK version 7u79 with JCE unlimited strength policy extension
  - J2EE Application Server: JBOSS EAP version 6.4.0
  - Cryptographic module support software: Thales Security World Software version 11.72.02
  - Cryptographic support libraries: Bouncy Castle JCE version 1.54
  - Database driver: Oracle Instant Client and JDBC Driver version 12.1
- Cryptographic module:
  - Thales nCipher nShield Connect+ HSM with nCore firmware 2.55.1
- Relational Database Management System:
  - Oracle 11g or Oracle 12c (all editions supported from XE to Enterprise Edition).
- PKI components needed to support the signature process:
  - Certification Authority
  - Registration authority

The TOE does not directly communicate with the HSM; the TOE sends the cryptographic operation request to cryptographic module support software (HSM manufacturer proprietary) that implements the communications protocol with the HSM. The cryptographic module support software includes a PKCS#11 library, drivers and services for interacting with the HSM.

The diagram shown in Figure 2 depicts the logical architecture of the components belonging the TOE interacting with the environment parts that are needed for the correct operation of the TOE.

2.4. TOE description

2.4.1 TOE definition

Physical scope

The TOE is software where all the components belonging the TOE are included and are delivered in a single file (***ssa.ear***) from version 1.1.8 specified in the software package.

The TOE is delivered together with the following guidance documents and files:

Title	Filename	Version	Description
AGD_PRE: PREPARATIVE PROCEDURES	AGD_PRE.pdf	2.12	Installation guide document.
AGD_OPE: OPERATIONAL PROCEDURES	AGD_OPE.pdf	1.12	User and administration guide document.
ADV_FSP: APPLICATION FUNCTIONAL SPECIFICATION	ADV_FSP.pdf	2.12	TOE functional specification document, includes the TOE's API description for developers.
	ssa_data.zip	1.1.8	Installation and configuration scripts and files.

Table 1 - TOE guidance documents and files

The TOE, the guides and the installation files may be distributed by email or by FTP when the ANCERT's personnel in charge of the TOE installation does not have access to configuration management system where the TOE releases are published.

Logical scope

The TOE is composed of the following components sub-set as part of the global solution:

- REST API modules: provide a REST API to remote applications, including:
  - Signer API, for SCA / CloudKSP applications.
  - RA API, for the Registration Authority
  - Administrative API, to perform administrative operations, e.g. with the Command Line Interface.
- The REST modules do not contain any business logic, which is provided by the SSA services and kernel modules.
- SSA services modules: implement the TSFIs business logic:
  - Registration Authority services.
  - Signer services.
  - Administrative services.
- SSA kernel modules: reusable modules providing security and other business functionalities. The kernel modules are invoked by the SSA service modules in the TSFIs implementation.
  - Config module: manages and stores the TOE configuration data.

- Common module: provides common components to other kernel modules, like exception handling, data structures and data formatting and zeroization functions.
- SecureDB module: provides basic primitives for storing and retrieving objects in a relational database, granting their authenticity and integrity. This service is invoked by the DB and Audit modules.
- DB module: manages the storage of TOE data in the database.
- Audit module: provides secure audit functionalities to the TOE, ensuring that individual audit records and the full audit trail could not be tampered.
- SSAService module: manages the system startup, shutdown and initialization and keeps the TOE operational status.
- AA module: provides authentication an authorization services, checking the username, password and role for the privileged users (administrators, operators and auditors) and performing certificate validation for unprivileged users (registration authorities and SCA applications).
- SAP module: in charge of processing the Signature Activation Protocol and authorizing the activation of the Signatory's key within the HSM.
- QSCDev module: performs the delegated cryptographic operations on the HSM making calls to the HSM's PKCS#11 library.

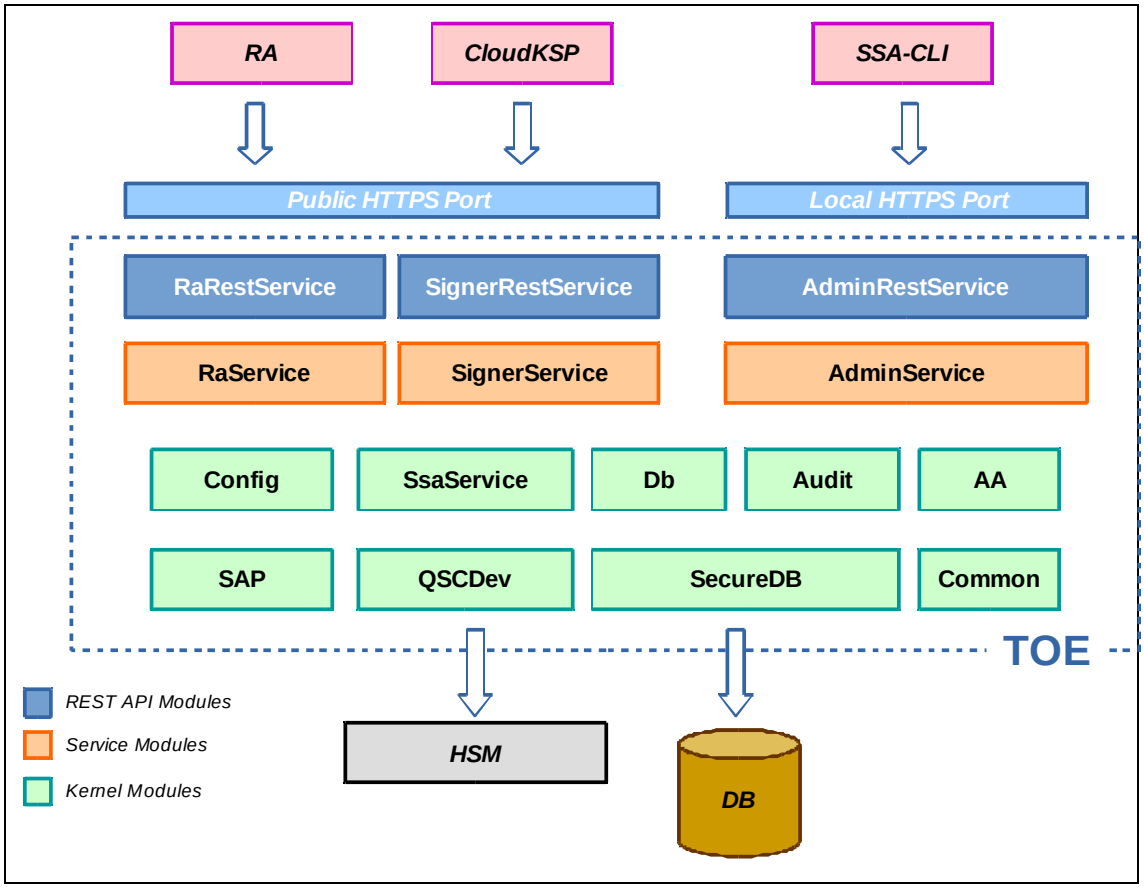


Figure 2 - TOE logical architecture

2.4.2 Signature Activation Protocol

The SSA requires two-factor authentication from the Signer to activate its SCD. The two-authentication factors are something the user knows (the SAD PIN) and something the user has under his sole control (a private key (Akr) in his SAA).

The SAP is a unique SAD message transmitted from the SAA to the TOE through the CloudKSP in which both authentication factors are sent together with the DTBSR.

The SAD message (Figure 3) is created by the SAA as follows:

- The SAA asks the Signer to input his SAD PIN.
- The SAA generates a symmetric session key (PINks).
- The SAD PIN typed by the Signer is encrypted with PINks.
- The session key is encrypted using a public key (PINku). The resulting ciphered message is named the SAD PIN envelope.
- The SAD message is composed joining together the DTBSR, the SAD PIN envelope and the encrypted SAD PIN.
- The SAD message is signed with the Signers' authentication private key (Akr).

The private key PINkr corresponding to PINku is managed by the TOE allowing the recovery of the SAD PIN sent to the SSA.

The public key Aku corresponding to Akr is sent to the SSA in the Signer's key pair creation operation and is stored as an SCD attribute allowing the SSA to verify the SAD signatures.

In order to grant sole control over the SCD the private key is generated inside the boundaries of a HSM an exported to a DB for its storage wrapped using a symmetric key derived from the Signer's SAD PIN and a key stored in the HSM. In order to perform any operation involving the SCD the SSA validates the SAD message signature and tries to activate the private key inside the HSM unwrapping the protected SCD with the SAD PIN supplied by the Singer in the SAP.

```
Operations:
C(M, K) := Cipher message M with key K, symmetric cipher
E(M, K) := Cipher message M with key K, asymmetric cipher
S(M, K) := Sign message M with key K
Message:
SAD := DTBSR | C(SAD PIN,PINks) | E(PINks,PINku) | S(DTBSR | C(SAD PIN,PINks) | E(PINks,PINku), Akr)
Message parts:
“SAD PIN envelope” := C(SAD PIN, PINks)
“Encrypted SAD PIN” := E(PINks, PINku)
```

Figure 3 - SAD message details

3. Conformance claim

3.1. CC conformance claim

This TOE conforms to Common Criteria version 3.1 Revision 5, in particular with the following parts:

- Functional requirements of Part 2 extended.
- Assurance requirements of CC Part 3.

This TOE's and ST's PP and package claim is stated in the following sub sections.

3.2. PP and package claim

3.2.1 PP claim

This security target does not claim conformance with any protection profile.

3.2.2 Package claim

This security target claims conformity with the EAL4 assurance package augmented with the AVA_VAN.5 and ALC_FLR.2 components.

3.2.3 Conformance rationale

The assurance level of EAL4 is considered to be most appropriate for this type of TOE since it is intended to defend against attacks that can be made given the assumptions, organizational security policies and the threats defined in this document.

4. Security problem definition

4.1. TOE assets

The following assets are under control of the TOE and need to be protected:

Signature creation data (SCD): private key used to sign data.

Signature requests: data used to request a signature operation including:

- **DTBS**: all data to be signed as well as any signature attributes that are bound together with the data as the input of the cryptographic algorithm to be used by the signature.
- **SAD**: (signature activation data) data used to activate the signature process that is uniquely known by the Signer.

Signature data: data as a result of the signature process that are the representation of the DTBS using the SCD.

Authentication data: authentication data from applications or users that request services from the TOE: certificates from applications or users or external services data.

Configuration data: configuration data of the TOE including configuration parameters of the users management, keys of the TOE used for the correct operation of it and parameters related to the communication with the DB and HSM.

Signer's data: keys and user's data under TOE management during the signature process.

Audit data: audit records generated by the TOE.

4.2. TOE users

The TOE has the following sets of users that can perform operations over or using the TOE.

4.2.1 Administrative users

Users that can manage the TOE through management operations over it, change the configuration of it, change the behavior of the TOE and access audit logs.

Administrative users access the TOE through the Administrative interfaces and are assigned to the following roles, depending on the privilege level that are assigned to them:

- **Security Officer**: having overall responsibility for administering the implementation of the security policies, practices and have access to security related information having overall responsibility for administering the implementation of the security policies and practices.
- **Administrators:** are authorized to install, configure and maintain the TOE but with controlled access to security-related information.
- **Operators:** are responsible for operating the TOE on a day-to-day basis and are authorized to perform system backup and recovery.

- **Auditors:** are authorized to view archives and audit logs of the TOE for the purposes of auditing the operations of the system in line with security policy.

Security officers and system administrators are privileged system users.

System operators and system auditors have privileged roles but are not able to administer or configure the TOE.

4.2.2 Registration Authority Operators

The Registration Authority (RA) is the entity that establishes, verifies and guarantees the identity of the signer to the trusted service provider (TSP). RA Operators connect to the TOE through a RA application which provides the role named **RA** to these users.

TSP will trust in the RA to perform the steps related to registering of the signer to correctly assign the certificates.

4.2.3 Signers

Users that request signature operations to the TOE through the signer interface using the data in the TOE and provides the data needed to perform the operation, including the activation data.

The Signer connects to the TOE through a CloudKSP application that acts as a reverse proxy forwarding the DTBS requests from the SCA and the SAD from the Signer's SAA to the TOE. The CloudKSP application provides the role named **CloudKSP** to the Signer users.

4.2.4 System

Some operations performed by the TOE without any user interaction, like internal components startup and shutdown or self protection checks, generate events that shall be audited. The username "SYSTEM" is assigned as the event source for the events of the aforementioned category.

4.3. Threats

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

- **External agent**: attackers who are not TOE users that have neither credentials nor access to the TOE or environment and whose main goal is accessing the signature creation data and counterfeit digital signature.
- **Internal agent**: attacker belonging to administrative users and having access to the TOE or the environment. These agents could make use of privileged information on the TOE to impersonate a signer in a signing procedure or elevate their privileges to manage the system.

Threads for the TOE are described in the table below:

THREAT	DESCRIPTION
T.ACCESS_CONTROL	External agent accessing the management of the TOE and performing not allowed operations.
T.COUNTERFEIT	External agent accessing to signature services and using SCD to perform signatures on behalf of the legitimate user.
T.DTBS_MODIFICATION	External agent modifies the data to be signed or their representation (DTBS or DTBS/R) used by the TOE in the way that the signed data is not the same that the signer sent to the TOE for being signed.
T.SD_MODIFICATION	External agent modifies the signed data (SD) in order to have new signed data that are not detected by the signature verification.
T.SAD_ACCESS	External agent accesses to the authentication data or signature activation data of the signers and is able to generate a signature without the signer having authorized the operation.
T.SCD_ACCESS	Internal agent access to signature creation data (SCD) out of the TOE or the environment and is able to generate a signature without the signer having authorized the operation.
T.USERS_DATA_MOD	External or internal agent without privileges modifies the signer's data to assign the SCD to another signer.
T.CONF_MODIFICATION	External or internal agent without privileges modifies the TOE configuration data to modify the privileges or the communication with the environment.
T.AUDIT_MODIFICATION	External or internal agent modifies the information recorded by the auditory data or generates invalid auditory information recorded as actual information.
T.BBDD_DATA	External or internal agent generates data in the database coming from another TOE or coming from a misconfiguration of the proper database that are taken by the TOE as valid data.

Table 2 - Threats

4.4. Organizational policies

The following organizational security policies are defined:

OSP	DESCRIPTION
P.CERTIFICATE	The certificates generated to be used in the TOE are trusted and according to eIDAS Art.3:14, Art.3:15, Annex I and to the policy for certificate generation of the TSP.
P.SIGNATURE_DATA	The signature creation data related to the DTBS or DTBSR used by the TOE are under control of the signer and allows detecting subsequent modifications.
P.REGISTRY	The identity of the holder is checked through a secure identification procedure before registering.
P.SIGNER_DATA	User data and certificates for accessing the TOE services by the signature creation applications and the related authentication data will be securely maintained during the signature procedure.
P.CONFIGURATION	The TOE is installed and configured by following the guidance's provided by the vendor.
P.ALERT	Alerts received during the authenticity checking of data stored in the database will be reviewed by the authorized personnel.
P.HSM	The hardware security module provides security features enough to ensure the robustness of the cryptographic operations.
P.ROL_GRANULARITY	The administrative users are related to a unique role so that not all the operations in the TOE and the environment are not in charge of a single administrator.
P.AUDIT_EXPORTATION	The auditory data are periodically exported from the database and are securely stored by authorized personnel by using secure means.
P.BACKUP	The TOE data necessary to perform a recovery of the system are periodically backed up and securely stored by authorized personnel by using secure means.
P.SIGN_ALGORITHMS	It is established the use of asymmetric cryptographic algorithms and key sizes recommended by "ETSI/TS 119 312" [ESI312] for hashing and signing.

P.ENCRYPTION_ALGORITHMS	It is established the use of cryptographic symmetric algorithms and key sizes recommended by "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms" [SOGCRYPT] for data encryption.

Table 3 - Organizational policies

4.5. Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE.

The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance.

The following table lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

ASSUMPTION	DESCRIPTION
A.TSP	The certification authority and TSP that issues certificates uses practices and methodology according to the approved certification policy.
A.SCA	The SCA used to generate DTSB or DTBSR works properly and generates the data in a proper way to be used by the TOE.
A.ENVIRONMENT	The environment (DB, HSM, operating system, application server and all the devices involved) are properly installed and secure configured to ensure the protection of the TOE and TOE resources. Modifications on the data stored into the database can only be performed through the TOE. Regarding other maintenance operations (such as backups), they can be performed through the DBMS.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.SIGNERS	All the signers have knowledge enough to operate the TOE correctly and will follow the guidance's provided by the vendor.
A.RELIABLE_TIME	The operational environment provides a reliable time source
A.TRUSTED_ENV_SAA	The signature activation application must run in a trustworthy environment.

Table 4 – Assumptions

5. Security objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition.

The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

5.1. Security objectives for the TOE

SECURITY OBJECTIVE FOR THE TOE	DESCRIPTION
O.AUTHENTICATION	All the operations using the assets of the TOE shall be performed under authentication of the user involved.
O.ACCESS_CONTROL	The access to the TOE services shall be controlled by means of the related permissions. These permissions will be checked to authorize the execution of the operation.
O.SCD_CONFIDENTIALITY	The TOE ensures the confidentiality of the SCD by using the external HSM, through the cryptographic module support software, for signing key generation and usage. The SCD never leaves the HSM boundaries in plain text, when a SCD is not in use the TOE deactivates the key and securely stores the SCD outside the HSM boundaries in the database. In the database SCD confidentiality is ensured by the usage of strong cryptographic algorithms.
O.SCD_USAGE	The usage of the private key of the users is protected by means of the use of the SAD (a secret belonging each particular Signer) that are never stored in the TOE and the master key that cannot be exported from the HSM.
O.SCD_SVD	The TOE ensures the correspondence between the SVD and the SCD generated, including the handler of the pair SVD/SCD.

O.SECURE_SIGNATURE	The TOE by means of the external HSM, through the cryptographic module support software, will generate digital signature by strong cryptography algorithms. The SCD cannot be inferred from the signed data and the authenticity will be ensured by the usage of strong cryptographic algorithms.
O.DATA_INTEGRITY	The configuration data and user data can only be modified by authorized users with privileges enough. The integrity and authenticity of the configuration data and user data from the DB will be protected through the generation of HMAC value to ensure that has been generated by the TOE.
O.AUDIT_INTEGRITY	The integrity and authenticity of the audit data will be protected through the generation of HMAC value.
O.KEY_PROT	The TOE will keep the following keys value: - HMAC key used to verify the TOE configuration and audit logs and the - RSA private key used to decrypt the SAD PIN envelope used to transport encrypted PIN in the SAP. by the use of a keystore protected by a password.
O.SELFPROTECT	The TOE shall prevent the processing of any request from the Signers or the RA in the following situations: - Audit facilities are not available. - TOE configuration data has been tampered. - TOE audit log has been tampered.

Table 5 - Security objectives for the TOE

5.2. Security objectives for the operational environment

The following security objectives for the operational environment of the TOE are defined to implements technical and procedural measures to assist the TOE in correctly providing its security functionality:

SECURITY OBJECTIVE FOR THE OPERATIONAL ENVIRONMENT	DESCRIPTION
OE.PHYS_ACCESS	The TOE is installed in a restricted access environment under control of the administrative users that are in charge of control the physical access to the TOE.

OE.TOE_ACCESS	The IT environment shall provide mechanisms that control user's logical access to the TOE.
OE.TOE_PROTECTION	The IT environment shall protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification.
OE.NO_EVIL	The TSP using the TOE shall ensure that administrative users are non-hostile, appropriately trained and follow all administrative guidance.
OE.SECURE_COMMS	The operational environment shall provide a secure communication line between the TOE and the other devices used for the correct operation of the TOE, in particular the command line interface, the RA and the Cloud KSP using the TLS protocol. TLS communications channels are provided and managed in the JBOSS application server. The TOE communicates with the HSM making local calls to the PKCS#11 library provided by the HSM manufacturer (cryptographic module support software)..
OE.SVD_VALIDATION	The TSP will check the SVD validity with the proof of possession (PKCS#10) exported from the TOE before providing the appropriate certificate to the SVD.
OE.SCD_SVD	The HSM guarantees the quality of the pair SCD/SVD to ensure that the probability of generating two times the same SCD is negligible.
OE.CERTIFICATE_GEN	The registration authority request the TSP to generate the certificates according to eIDAS Art.3:14, Art.3:15, Annex I and EN 319 411 including the name of the signer, the SVD related to the SCD generated by means of the TOE and the signature of the TSP.
OE.AUT_DATA_PROT	The application requesting the authentication data will ensure the confidentiality and integrity of them until being sent to the TOE.
OE.DTBS_CORRECT	The DTBS and DTBSR provided by the users through the environment to the TOE are correctly formatted and are provided by a secure channel that ensures the confidentiality and integrity of these data.
OE.TOE_CONFIG	The guidance's to correctly configure and operate the TOE are available.

OE.SIGNER_ACCOUNT	Registration authority will check the identity of the signer and ensures the user to configure the SAD and will maintain the confidentiality and integrity of the data until sending to the TOE.
OE.SECURE_BACKUP	Periodic backups will be done and the environment will ensure the integrity and confidentiality of the stored data. The backups will contain the information enough to ensure the correct operation of the TOE and the environment (HSM and DB) after an eventual failure of the system.
OE.SECURE_HSM	The HSM used to perform signature among other cryptographic operations will maintain a high security level by fulfilling the following Common Criteria assurance level: • EAL4+AVA_VAN.5.
OE.VALIDATION_HMAC	The auditory and DB data will be periodically checked to find data that could be non-generated by the TOE.
OE.SIGNERS_OPER	The guidance's to correctly operate the TOE are available, including security warnings for keeping the VAD secured.
OE.ROLE_ASSIGNMENT	User's belonging to a particular role cannot be assigned to another role at the time.
OE.AUDIT_BACKUP	The procedure for backing up the audit data will be periodically executed by the authorized personnel and the resulting backup will be securely stored.
OE.SECURE_CRYPTO	The following algorithms will be used by the TOE and the environment to ensure the fulfillment of [ESI312]: • SHA-256 or higher for hashing on the DTBS. • RSA with key of 2048 bits or higher for signature. The following algorithms will be used by the TOE and the environment to ensure the fulfillment of [SOGCRYPT]: • AES with key of 128 bits or higher for data encryption and Signer key wrapping.
OE.RELIABLE_TIME	The operational environment shall provide a reliable time source.
OE. TRUSTED_ENV_SAA	The operational environment where the signature activation application runs must be trusted.

Table 6 - Security objectives for the operational environment

5.3. Security objectives rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target.

The table maps the threats and policies to the security objectives for the TOE:

	O.AUTHENTICATION	O.ACCESS_CONTROL	O.SCD_CONFIDENTIALITY	O.SCD_USAGE	O.SCD_SVD	O.SECURE_SIGNATURE	O.DATA_INTEGRITY	O.AUDIT_INTEGRITY	O.KEY_PROTECT	O.SELFPROTECT
T.ACCESS_CONTROL	X	X								X
T.COUNTERFEIT				X	X					
T.DTBS_MODIFICATION										
T.SD_MODIFICATION						X				
T.SAD_ACCESS							X			
T.SCD_ACCESS			X	X						
T.USERS_DATA_MOD		X								X
T.CONF_MODIFICATION		X								
T.AUDIT_MODIFICATION		X								
T.BBDD_DATA							X	X	X	
P.CERTIFICATE										
P.SIGNATURE_DATA			X	X	X	X				
P.REGISTRY					X					
P.SIGNER_DATA	X	X								
P.CONFIGURATION	X	X					X			
P.HSM										
P.ROLE_GRANULARITY										
P.AUDIT_EXPORTATION										
P.BACKUP										
P.SIGN_ALGORITHMS										
P.ENCRYPTION_ALGORITHMS										

Table 7 - Security objectives for TOE and threts / policies mapping

The table maps the threats, policies and assumptions to the security objectives for the operational environment:

	OE.PHYS_ACCESS	OE.TOE_ACCES	OE.TOE_PROTECTION	OE.NO_EVIL	OE.SECURE_COMMS	OE.SVD_VALIDATION	OE.SCD_SVD	OE.CERTIFICATE_GEN	OE.AUT_DATA_PROT	OE.DTBS_CORRECT	OE.TOE_CONFIG	OE.SIGNER_ACCOUNT	OE.SECURE_BACKUP	OE.SECURE_HSM	OE.VALIDATION_HMAC	OE.SIGNERS_OPER	OE.ROLE_ASSIGNMENT	OE.AUDIT_BACKUP	OE.SECURE_CRYPTO	OE.RELIABLE_TIME	OE. TRUSTED_ENV_SAA
T.ACCESS_CONTROL																	X				
T.COUNTERFEIT									X			X									
T.DTBS_MODIFICATION					X					X											
T.SD_MODIFICATION					X	X	X							X					X		
T.SAD_ACCESS					X						X										
T.SCD_ACCESS																					
T.USERS_DATA_MOD	X																				
T.CONF_MODIFICATION	X				X																
T.AUDIT_MODIFICATION	X				X																
T.BBDD_DATA															X						
P.CERTIFICATE						X	X	X													
P.SIGNATURE_DATA						X	X	X		X				X							
P.REGISTRY									X			X				X					
P.SIGNER_DATA					X				X							X					
P.CONFIGURATION	X			X	X						X										
P.HSM														X							
P.ROLE_GRANULARITY																	X				
P.AUDIT_EXPORTATION																		X			
P.BACKUP				X									X								
P.SIGN_ALGORITHMS																			X		
P.ENCRYPTION_ALGORITHMS																			X		
A.TSP						X		X													
A.SCA									X	X											
A.NO_EVIL				X																	
A.ENVIRONMENT	X	X	X	X	X						X		X								
A.SIGNERS																X					
A.RELIABLE_TIME																				X	
A.TRUSTED_ENV_SAA																					X

Table 8 - Security objectives for the operational environment and threats / policies / assumptions mapping

T.ACCESS_CONTROL: The user is authenticated (O.AUTHENTICATION) and its privileges are checked (O.ACCESS_CONTROL) before performing any action.

In addition the users in the system cannot access to all operations in the TOE (OE.ROLE_ASSIGNMENT).

External applications con not perform any action in the TOE if configuration data tampering is detected (O.SELFPROTECT).

T.COUNTERFEIT: The SCD cannot bring out of the control of the TOE and can only be activated within the TOE boundary (O.SCD_USAGE). Also, for avoiding the unauthorized use of the SCD by an attacker, the SCD and SVD are linked in a secure way by the TOE (O.SCD_SVD, OE.SIGNER_ACCOUNT) and the user is forced to establish a password for their protection (O.SCD_USAGE).

In addition, the data managed by the signature creation application are verified before sending the data to the TOE (OE.AUT_DATA_PROT).

T.DTBS_MODIFICATION: The data to be signed are sent to the TOE through a secure channel ensuring the confidentiality and integrity of the data (OE.SEC_COMMS) and are verified to ensure that has not been modified by the signature creation application (OE.DTBS_CORRECT).

T.SD_MODIFICATION: Counterfeiting the signature is countered by the use of strong algorithms (O.SECURE_SIGNATURE) and keys ensuring the integrity of the results (OE.SECURE_CRYPTO). Also the data resulting is transmitted through secure channels that ensure the confidentiality and integrity of the data (OE.SECURE_COMMS) and avoids the unauthorized access.

The signature can also be verified (OE.SVD_VALIDATION) with the related verification data related to it that guarantees the correspondence (OE.SCD_SVD).

The particular signature operation is carried by the HSM with strong ciphering mechanisms (OE.SECURE_HSM).

T.SAD_ACCESS: The access to authentication data and protection passwords is protected through the secure channel used to transmit the data (OE.SECURE_COMMS) in the way that only the authorized user and the TOE can access to the data.

The configuration of the TOE is ensured to be correctly performed by following the guidance's (OE.TOE_CONFIG) and the TOE is verified to be correctly configured by checking the authenticity of the data to ensure that the configuration parameters are the correct generated by the TOE (O.DATA_INTEGRITY).

T.SCD_ACCESS: The signature creation data are protected from disclosure by ensuring that the SCD cannot leave the HSM (O.SCD_CONFIDENTIALITY) and ensuring that the only person accessing the SCD is the proprietary of the key (O.SCD_USAGE).

T.USERS_DATA_MOD: It is defined an access control on the users data in the way that uniquely the authorized users can modify the data belonging the TOE (O.ACCESS_CONTROL) or accessing to the management over the environment (OE.PHYS_ACCESS). The access and modification of the data through an unauthorized access to the DB is protected.

External applications con not perform any action in the TOE if configuration data tampering is detected or the actions cannot be audited (O.SELFPROTECT).

T.CONF_MODIFICATION: An access control is defined for the configuration of the TOE. The configuration is protected for being modified by unauthorized users (O.ACCESS_CONTROL) and the environment configuration (OE.PHYS_ACCESS).

The configuration data are transmitted through secure channels to ensure the confidentiality and integrity of them (OE.SECURE_COMMS).

T.AUDIT_MODIFICATION: Audit data cannot be generated by unauthorized users as they have no access to the TOE functionality (O.ACCESS_CONTROL) or accessing to the DB in the environment (OE.PHYS_ACCESS).

The configuration data are transmitted through secure channels to ensure the confidentiality and integrity of them (OE.SECURE_COMMS).

T.BBDD_DATA: Data coming from the DB –configuration and users data- are checked to ensure that are generated by the TOE and has not been modified (O.DATA_INEGRITY) and also the auditory data (O.AUDIT_INTEGRITY) by means of HMAC checking. The particular HMAC key is protected from unauthorized access (O. KEY_PROT).

Also the alert mechanism is implemented on auditory data to avoid the usage of not genuine data by the TOE (OE.VALIDATION_HMAC).

P.CERTIFICATE: Certificates are generated by the environment according to eIDAS Art.3:14, Art.3:15, Annex I and EN 319 411 (OE.CERTIFICATE_GEN) ensuring that the certificate is issued from the SVD given by the TOE (OE.SVD_VALIDATION) and the correct correspondence with the SCD (OE.SCD_SVD).

P.SIGNATURE_DATA: The signature process is based on advanced electronic signature (a qualified signature based on a qualified and valid certificate). Due to this, the key pair generated is guaranteed to be securely generated and unique (O.SCD_SVD, OE.SVD_VALIDATION, OE.CERTIFICATE_GEN, OE.SECURE_HSM and OE.SCD_SVD).

The private key confidentiality is protected throughout the signature process and at rest (O.SCD_ CONFIDENTIALLITY) and the signer sole control over the key is granted by O.SCD_USAGE. The signature process robustness is granted by O.SECURE_SIGNATURE and the integrity of the data to be signed by OE.DTBS_CORRECT.

P.REGISTRY: The signer is registered through the RA, so that the identity of the signer is verified before generating the key pair and the signature activation data (OE.SIGNER_ACCOUNT) and the data is securely transmitted to the TOE (OE.AUT_DATA_PROT).

The certificate is requested by the RA to the CA for sending it to the TOE for linking with the private key, which ensures the correspondence of the SCD to the SVD (O.SCD_SVD).

The securely maintenance of the activation data is ensured by the procedures defined in the guidance documentation (OE.SIGNERS_OPER).

P.SIGNER_DATA Certificates for accessing the TOE are securely maintained to protect their confidentiality. The signature creation applications access the TOE through certificate authentication (O.AUTHENTICATION, O.ACCESS_CONTROL).

Access to the TOE is performed through secure channel to avoid the disclosure of the authentication data (OE.SECURE_COMMS, OE.AUT_DATA_PROT).

Configuration of the signature creation application is ensured by the procedures defined in the guidance documentation (OE.SIGNERS_OPER).

P.CONFIGURATION: The configuration of the TOE is performed correctly by following the guidance's provided (OE.TOE_CONFIG) by non-hostile and appropriately trained administrators (A.NO_EVIL) and this process has to be done after authentication and access control of the user (OE.PHYS_ACCESS, O.AUTHENTICATION, O.ACCESS_CONTROL, O.DATA_INTEGRITY) over a secure channel (OE.SECURE_COMMS).

The authenticity of the configuration data is ensured by the HMAC value defined for it (O.CONF_INTEGRITY).

P.HSM: Signature creation device fulfills the requirement on strength for cryptographic operations to ensure the robustness of the algorithms used (OE.SECURE_HSM).

P.ROLE_GRANULARITY: Users profiles are assigned not to allow one user have access to all operations in the TOE and the profiles that the user can have are defined (OE.ROL_ASSIGNMENT).

P.AUDIT_EXPORTATION: The administrator will determine the exportation of the data and the secure storage of them (OE.AUDIT_BACKUP).

P.BACKUP: Configuration data are periodically backed up to ensure the early recovery of the system in case of a critical failure (OE.SECURE_BACKUP). The procedures backup all necessary data to ensure the correct recovery of the entire system. Backups are performed by appropriately trained personnel following all the administrative guidance (A.NO_EVIL).

P.SIGN_ALGORITHMS: Secure algorithms are only used according to the parameters defined in technical specification [ESI312] (OE.SECURE_CRYPTO).

P. ENCRYPTION_ALGORITHMS: Secure algorithms are only used according to the parameters defined in [SOGCRYPT] (OE.SECURE_CRYPTO).

A.TSP: The TSP protects the authenticity of signer and the public key by generating and signing the certificates. The TSP validates the SVD from the TOE (OE.SVD_VALIDATION) and generates the certificate (OE.CERTIFICATE_GEN).

A.SCA: The signer uses trusted SCAs that generate the DTBS/DTBSR adequately to be sent to the TOE. The application is authenticated against the TOE in the way that only trusted SCAs can use the services provided by the TOE (OE.AUT_DATA_PROT).

Application sends the data to the TOE through the secure channel and have the data of the signature performed (OE.DTBS_CORRECT).

A.NO_EVIL: This assumption is directly mapped to OE.NO_EVIL which states that TSP using the TOE shall ensure that administrative users are non-hostile, appropriately trained and follow all administrative guidance.

A.ENVIRONMENT: The environment can only be accessed by having the correct authorization and after the established physical and logical environment (OE.PHYS_ACCESS, OE.TOE_ACCESS) controls that guarantees that the TOE can only be managed by administrative users.

The environment establishes proper logical controls to protect the TOE and the TOE resources from external interference, tampering, or unauthorized disclosure and

modification (OE.TOE_PROTECTION). The environment is configured and managed by non-hostile administrators, appropriately trained and following all administrator guidance (OE.NO_EVIL).

The administrative users configure the TOE according to the specification and documentation of the TOE (OE.TOE_CONFIG) and also the secure channels that ensure the communications with third parties (OE.SECURE_COMMS).

Configuration data are periodically backed up to ensure the early recovery of the system in case of a critical failure (OE.SECURE_BACKUP).

Modifications on the data stored into the database can only be performed through the TOE. Regarding other maintenance operations (such as backups), they can be performed through the DBMS.

A.SIGNERS: All Signers can operate the TOE in a secure manner by following the procedures defined in the guidance documentation (OE.SIGNERS_OPER).

A.RELIABLE_TIME: The reliable time source is provided directly by the operational environment (OE.RELIABLE_TIME).

A.TRUSTED_ENV_SAA: The signature activation application runs in a trustworthy environment (OE.TRUSTED_ENV_SAA).

6. Extended components definition

6.1. Cryptographic operation (FCS_COP)

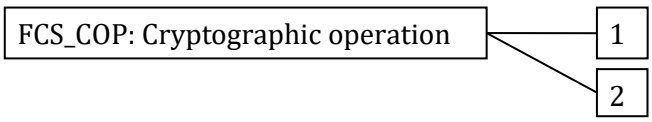
Following the class **FCS: Cryptographic support** defined in CC Part 2 belonging to Common Criteria v3.1 R5 is extended to adapt the security functional requirements of the TOE related to the cryptographic operations used by it.

Extending the class **FCS: Cryptographic support** is justified due to there is no component that describes the cryptographic operations invoked by the TSF that are actually performed in the boundary of an external device.

6.1.1 Family behaviour

Family **Cryptographic operation (FCS_COP)** is extended to add a new level **FCS_COP.2** that describes the delegation of the cryptographic operations to a signature creation device (SCDev) evaluated and certified in accordance to the evaluation criteria defined in ISO/IEC 15408, and with the evaluation methodology laid out in ISO/IEC 18045 "Methodology for IT security evaluation", at a minimum evaluation assurance level of EAL4+AVA_VAN.5.

6.1.2 Components leveling



FCS_COP.2 Delegated cryptographic operation, requires a cryptographic operation to be performed into an external SCDev evaluated and certified Common Criteria EAL4+AVA_VAN.5.

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 SCDev evaluated and certified Common Criteria EAL4+AVA_VAN.5 to perform [**assignment:** cryptographic operations].

6.2. Stored data confidentiality (FDP_SDC)

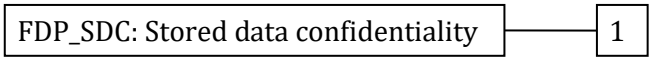
Following the class **FDP: User data protection** defined in CC Part 2 belonging to Common Criteria v3.1 R5 is extended to adapt the security functional requirements of the TOE related to the protection of the user data stored in it.

Extending the class **FDP: User data protection** is justified due to there is no component that describes confidentiality of the stored data. Therefore it is created the family **Stored data confidentiality (FDP_SDC)** that guarantees the confidentiality of the user data stored trough the TSF.

6.2.1 Family behavior

This family provides requirements that address protection for confidentiality of user data while it is stored within containers controlled by the TSF. Confidentiality may affect user data stored in memory, or in a storage device.

6.2.2 Component leveling



This family consists of only one component, FDP_SDC.1 Basic confidentiality of user data, addresses the protection from disclosure of user data stored.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no auditable events foreseen.

FDP_SDC.1: Stored data confidentiality

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SDC.1.1 The TSF shall provide confidentiality on the [**assignment:** user data stored].

6.1. User data correspondence (FDP_UDC)

Following the class **FDP: User data protection** defined in CC Part 2 belonging to Common Criteria v3.1 R5 is extended to adapt the security functional requirements of the TOE related to the association and correspondence of the user data.

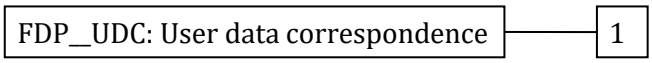
Extending the class **FDP: User data protection** is justified due to there is no component that describes the guarantee of the relationship of the user data providing integrity check over the particular relation. Therefore it is created the family **User data correspondence**

(FDP_UDC) that guarantees the correspondence between the data of the user e.g. the signature creation data (SCD) and signature verification data (SVD).

6.1.1 Family behavior

This family provides requirements that address correspondence of user data controlled by the TSF.

6.1.2 Component leveling



This family consists of only one component, FDP_UDC.1 Addresses the correspondence of user data.

Management: FDP_UDC.1

There are no management activities foreseen.

Audit: FDP_UDC.1

There are no auditable events foreseen.

FDP_UDC.1: User data correspondence

Hierarchical to: No other components

Dependencies: No dependencies

FDP_UDC.1.1 The TSF shall guarantee the correspondence between the SVD exported and the SCD generated by the TOE.

FDP_UDC.1.2 The TSF shall guarantee the correspondence between the Certificate imported and the SCD generated by the TOE.

7. Security requirements

The following typographical distinctions for the required operations have been used:

- Assignments: [**assignment:** <text>]
- Selections: [**selection:** <text>]
- Refinements: *Refinement: <text>*
- Iterations: /<iteration>

7.1. Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class and identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

7.1.1 Class FAU: Security audit

FAU_GEN.1: Audit data generation

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:** not specified] level of audit; and
c) [**assignment:** The events listed in Table 9].

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 9].

EVENT	CODE	DESCRIPTION	ADDITIONAL INFO
SYSTEM_INITIALIZED	00	System initialization, first record in the audit trail.	
MODE_CHANGED	01	Operational mode changed.	Old operational mode, new operational mode.
LOGIN	02	Administrative user logged in	
LOGOUT	03	Administrative user logged out	
SERVICESTART	04	Administrative user requested the TOE to start processing requests.	
SERVICESTOP	05	Administrative user requested the TOE to stop processing requests.	

USERADD	06	Administrative user added.	New username and role granted to the user.
USERDEL	07	Administrative user deleted.	Username.
USERPASSWD	08	Administrative user's password changed.	Username.
CERTADD	09	Client application added.	Certificate fingerprint, role granted.
DELCERT	10	Client application deleted.	Certificate fingerprint.
CACERTADD	11	Trusted system CA added.	Certificate fingerprint.
DELCACERT	12	Trusted system CA removed.	Certificate fingerprint.
PUSHCONFIG	13	Local SSA configuration pushed to remote database.	Configuration ID.
PULLCONFIG	14	Configuration stored in database pulled	Configuration ID.
CREATEKEYPAIR	15	Signer's SCD/SVD created.	SCD ID
ACTIVATESIGNATURE	16	Signer's SCD activated (status=ACTIVE).	SCD ID
DEACTIVATESIGNATURE	17	Signer's SCD deactivated (status=DEACTIVATED).	SCD ID
SIGNATURE	18	Signature created with the Signer's SCD.	SCD ID
GETCURRENTCONFIG	19	Administrative user requested to review the local configuration.	
GETDBCONFIG	20	Administrative user requested to review the remote configuration stored in the database.	Configuration ID.
CHANGESIGNERPIN	21	Signer's SAD PIN changed.	SCD ID
AUDITSTART	22	Audit service started.	
AUDITSTOP	23	Audit service stopped.	
PINBLOCKED	24	Signer's SCD blocked, after the unsuccessful authentication attempts limit is reached. (status=LOCKED)	SCD ID
BADPIN	25	Signer sent a wrong SAD PIN.	
CREATETW4S	26	First SSA configuration stored in the database.	
SENDALERT	27	Alert sent	
AUDITGENERATIONLOGSTART	28	Audit log export stat	
AUDITGENERATIONLOGFINISHED	29	Audit log export finished	

GETSERVERMODE	30	Administrative user queried the current system operational mode	System operational mode
GETSSAVERSION	31	Administrative user queried the SSA version	SSA version

Table 9 - TOE Events audited

FAU_GEN.2: User identity association

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

FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide [**assignment:** administrative users with AUDITOR] role with the capability to read [**assignment:** all data] from the audit records.

FAU_SAR.2: Restricted audit review

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

FAU_SAR.3: Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**assignment:** methods of selection] of audit data based on [**assignment:** date and time of event, type of event, identity of the entity and success or failure of the audited event].

FAU_STG.1: Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

Application note: this is only for internal audit trail not for the records stores in the database.

FAU_STG.1.2 The TSF shall be able to [**assignment:** detect] unauthorised modifications to the stored audit records in the audit trail.

Application note: the audit trail integrity and audit records authenticity is checked on the TOE start-up, periodically during the TOE execution (every 12 hours), on each time an auditor requests an audit log search or export operation, and also when an auditor requests an audit trail integrity check by demand.

FAU_STG.4: Prevention of audit data loss

Refinement: ***FAU_STG.4.1*** *The TSF shall* ***[selection:*** *prevent audited events]* *and* ***[assignment:*** *none] if the audit trail is not available, whatever it is the root cause of the unavailability (full audit trail or other database errors).*

7.1.2 Class FCO: Communication

FCO_NRO.2: Enforced proof of origin

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [**assignment:** CSR (PKCS#10)] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [**assignment:** SCD] of the originator of the information, and the [**assignment:** CSR (PKCS#10)] of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to the [**assignment:** recipient] given [**assignment:** electronic signature using SCD].

7.1.3 Class FCS: Cryptographic support

FCS_CKM.3: Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [**assignment:** access to the cryptographic HMAC key and the PINkr key] in accordance with a specified cryptographic key access method [**assignment:** JKS] that meets the following: [**assignment:** JKS].

FCS_COP.1/SAD PIN decipher: Cryptographic operation

FCS_COP.1.1/SAD PIN decipher: The TSF shall perform [**assignment:** symmetric deciphering] in accordance with a specified cryptographic algorithm [**assignment:** AES/GCM] and cryptographic key sizes [**assignment:** AES-128] that meet the following: [**assignment:** FIPS PUB-197, NIST-SP800-38D].

FCS_COP.1/SAD PIN envelope decipher: Cryptographic operation

FCS_COP.1.1/SAD PIN envelope decipher: The TSF shall perform [**assignment:** deciphering] in accordance with a specified cryptographic algorithm [**assignment:** RSA OAEP with SHA1 and MGF1 padding] and cryptographic key sizes [**assignment:** RSA-2048] that meet the following: [**assignment:** PKCS#1v2].

FCS_COP.1/HMAC: Cryptographic operation

FCS_COP.1.1/HMAC: The TSF shall perform [**assignment:** calculation/verification of 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:** RFC 2104].

FCS_COP.1/SAD signature verification: Cryptographic operation

FCS_COP.1.1/SAD signature verification: The TSF shall perform [**assignment:** verification of the SAD signature] in accordance with a specified cryptographic algorithm [**assignment:** RSA with SHA-256 hashing] and cryptographic key sizes [**assignment:** RSA-2048, SHA-256] that meet the following: [**assignment:** PKCS#1v2, FIPS PUB 180-4].

FCS_COP.2/SCD-SVD generation: Delegated Cryptographic operation

FCS_COP.2.1/SCD-SVD generation: The TSF shall invoke an external SCDev evaluated and certified Common Criteria EAL4+AVA_VAN.5 to perform [assignment: *generateKeyPair* (RSA-2048), *deriveKey* (AES-CMAC-128), *wrapKey* (AES-CBC-128), *destroyObject*]

FCS_COP.2/SCD activation: Delegated Cryptographic operation

FCS_COP.2.1/SCD activation: The TSF shall invoke an external SCDev evaluated and certified Common Criteria EAL4+AVA_VAN.5 to perform [**assignment:** *deriveKey* (AES-CMAC-128), *unwrapKey* (AES-CBC-128), *sign*, *destroyObject*]

FCS_COP.2/SAD PIN change: Delegated Cryptographic operation

FCS_COP.2.1/SAD PIN change: The TSF shall invoke an external SCDev evaluated and certified Common Criteria EAL4+AVA_VAN.5 to perform [assignment: *deriveKey* (AES-CMAC-128), *unwrapKey* (AES-CBC-128), *wrapKey* (AES-CBC-128), *destroyObject*]

7.1.4 Class FIA: Identification and authentication

FIA_UID.2: User identification before any action

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

FIA_UAU.2: User authentication before any action

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

FIA_UAU.6: Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**assignment:** the user has previously logged out].

FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [**selection:** [**assignment:** three]] unsuccessful authentication attempts occur related to [**assignment:** consecutive SCD activation attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**selection:** met], the TSF shall [**assignment:** mark the SCD as blocked (PIN_BLOCKED)].

FIA_SOS.1: Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment:** administrative password complexity policy]

7.1.5 Class FDP: User data protection

FDP_ACC.1/Administrative: Subset access control

FDP_ACC.1.1/Administrative: The TSF shall enforce the [**assignment:** administrative users control policy SFP] on [**assignment:**

Subjects: Administrative users,

Objects: administrative user accounts, application accounts, audit data, TOE configuration data,

Operations: TOE initialization, add, remove administrative user accounts, change user's passwords, add, remove application accounts, add, remove trusted CAs, push and pull

TOE configuration data to / from the database, query configuration data, query audit data].

FDP_ACC.1/Signer: Subset access control

FDP_ACC.1.1/Signer: The TSF shall enforce the [**assignment:** signers control policy SFP] on [**assignment:**

Subject = Signers,

Object = Signers keys (SCD/SVD), signature activation data.

Operations = digital signature, SAD PIN change].

FDP_ACC.2/Applications: Complete access control

FDP_ACC.2.1/Applications: The TSF shall enforce the [**assignment:** applications' control policy SFP] on [**assignment:**

Subjects = client applications (RA, CloudKSP) accessing the TSF's REST services,

Objects = Signers keys (SCD/SVD), signature activation data]

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

FDP_ACC.2.2/Applications: The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/Management: Security attribute based access control

FDP_ACF.1.1/Management: The TSF shall enforce the [**assignment:** administrative users control policy SFP] to objects based on the following: [**assignment:**

- Objects:
  - Administrative user accounts.
  - Application accounts.
  - TOE configuration data.
  - TOE operational status.
  - Audit data.
- Subjects:
  - Administrative users.
- Attributes from subjects:
  - User authentication data from user password.
  - User role].

FDP_ACF.1.2/Management: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:**

- From administrative users
  - Username is registered in the TOE and are related to the user in the TOE and password authentication is successful.
  - After authentication, the user has the role with authorization enough to execute the requested operations].

FDP_ACF.1.3/Management: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**assignment:**

- Dual access control (Administrator + Security Officer) for the following operations:
  - Add, remove or modify administrative users.
  - Add, remove authorized applications (RA or CloudKSP applications).
  - Assign roles to administrative users.
  - Add or remove trusted CA.
  - Push and pull TOE configuration data to / from the database].

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

FDP_ACF.1/Signature: Security attribute based access control

FDP_ACF.1.1/Signature: The TSF shall enforce the [**assignment:** signers control policy SFP] to objects based on the following: [**assignment:**

- Objects:
  - Signer keys (SCD/SVD), signature activation data.
- Attributes from objects:
  - Signature activation data from signer.
  - Certificate of the SCD to be used.
- Subjects:
  - Signers]

FDP_ACF.1.2/Signature: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:**

- Signer requesting digital signature:
  - Fulfill the policy described in FDP_ACF.1/Signer.
  - If authorization stage is fulfilled, authenticity of the signer holding the keys is determined by:
    - SAP request is verified with the user's SSA public key.
    - Only if the previous stage is completed with success and the signature token is ENABLED and not BLOCKED and its usage period is not expired, then the SCD will be activated within the HSM boundaries with the SAD PIN provided by the user in the SAP request and the HSM wrapping key. It this second phase is also completed with success private key access is granted.
    - After the signature operation, the SCD is deactivated again and a new activation is required for a new signature operation.
- Signer requesting the change of the password:
  - Fulfill the policy described in FDP_ACF.1/Signer.
  - If authorization stage is fulfilled, authenticity of the signer holding the keys is determined by:
    - SAD PIN change request is verified with the user's SSA public key.

- Only if the previous stage is completed with success and the signature token is ENABLED and not BLOCKED, then the SCD will be activated within the HSM boundaries with the current SAD PIN provided by the user in the request and the HSM wrapping key. It this second phase is also completed with success private key access is granted.
- The private key is protected with the new SAD PIN provided in the request and the HSM wrapping key.
- The SCD is deactivated again.].

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

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

FDP_ACF.1/Applications: Security attribute based access control

FDP_ACF.1.1/Applications: The TSF shall enforce the [**assignment:** applications control policy SFP] to objects based on the following: [**assignment:**

- Objects:
  - Signers keys (SCD/SVD), signature activation data
- Subjects:
  - RA and CloudKSP applications
- Attributes from subjects:
  - Application identity from the application certificate.
  - Application role].

FDP_ACF.1.2/Applications: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**assignment:**

- RA requesting key pair creation / activation / deactivation operations:
  - Fulfill the policy described in FDP_ACF.1/Applications.
  - Application authentication certificate is valid and it is associated to the required application role in the system configuration].
- CloudKSP requesting signature / PIN change operations:
  - Fulfill the policy described in FDP_ACF.1/Applications.
  - Application authentication certificate is valid and it is associated to the required application role in the system configuration].

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

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

FDP_ETC.2/CSR: Export of user data with security attributes

FDP_ETC.2.1/CSR: The TSF shall enforce the [**assignment:** applications control policy SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/CSR: The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/CSR: The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/CSR: The TSF shall enforce the following rules when user data is exported from the TOE: [**assignment:** SVD is exported using the PKCS#10 file format and signed with the SCD].

FDP_ITC.1/Certificate association: Import of user data without security attributes

FDP_ITC.1.1/Certificate association: The TSF shall enforce the [**assignment:** applications control policy SFP] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Certificate association: The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/Certificate association: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**assignment:** checking of the public key of the certificate with the related SVD generated by the TOE].

FDP_ITC.1/SSA public key: Import of user data without security attributes

FDP_ITC.1.1/SSA public key: The TSF shall enforce the [**assignment:** applications control policy SFP] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SSA public key: The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/SSA public key: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**assignment:** checking the private key proof of possession verifying a PKCS#10 signature].

FDP_RIP.1: Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**selection:** deallocation of the resource from] the following objects: [**assignment:** administrative users' passwords, signers' SAD PIN].

FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [**assignment:** integrity and authenticity errors] on all objects, based on the following attributes: [**assignment:** record signature (HMAC) field].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [**assignment:** change operational mode and prevent processing any request from the Signers and the RA].

FDP_SDC.1: Stored data confidentiality

FDP_SDC.1.1 The TSF shall provide confidentiality on the **[assignment:** SCD private key for signature].

FDP_UCT.1: Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the [**assignment:** signers control policy SFP] to [**selection:** receive] user data in a manner protected from unauthorised disclosure.

NOTE: *Signer SAD PIN shall be transmitted encrypted from the Signers' SAA to the SSA. Each time the SAD PIN is transmitted a new symmetric session key shall be generated in the SAA for SAD PIN encryption. SAD PIN encryption session keys shall be transmitted ciphered with a public key which corresponding private key shall be under the SSA sole control.*

FDP_UIT.1: Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the [**assignment:** signers control policy SFP] to [**selection:** receive] user data in a manner protected from [**selection:** modification] errors.

NOTE: *DTBSR and Signer SAD PIN shall be transmitted using signed messages.*

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [**selection:** modification] has occurred.

FDP_UDC.1: User data correspondence

FDP_UDC.1.1 The TSF shall guarantee the correspondence between the SVD and the SCD generated by the TOE.

FDP_UDC.1.2 The TSF shall guarantee the correspondence between the Certificate imported and the SCD generated by the TOE.

7.1.6 Class FMT: Security management

FMT_MSA.1/Accounts: Management of security attributes

FMT_MSA.1.1/Accounts: The TSF shall enforce the [**assignment:** administrative users control policy SFP] to restrict the ability to [**selection:** modify, delete, [**assignment:** create]] the security attributes [**assignment:** administrative accounts (Administrators, Operators, Security Officers and Auditors), application accounts (RA, CloudKSP)] to [**assignment:** administrative users with role Security Officer].

FMT_MSA.1/Create key: Management of security attributes

FMT_MSA.1.1/Create key: The TSF shall enforce the [**assignment:** applications control policy SFP] to restrict the ability to [**selection:** [**assignment:** creation of keys for signers]] the security attributes [**assignment:** SCD/SVD] to [**assignment:** authorized RA applications].

FMT_MSA.1/Activate key: Management of security attributes

FMT_MSA.1.1/Activate key: The TSF shall enforce the [**assignment:** applications control policy SFP] to restrict the ability to [**selection:** [**assignment:** activate / deactivate keys]] the security attributes [**assignment:** key activation status, key expiration] to [**assignment:** authorized RA applications].

FMT_MSA.1/Change SAD PIN: Management of security attributes

FMT_MSA.1.1/Change SAD PIN: The TSF shall enforce the [**assignment:** Signers control policy SFP] to restrict the ability to [**selection:** [**assignment:** modify the PIN for activation the SCD] the security attributes [**assignment:** SCD] to [**assignment:** Signers].

FMT_MSA.2: Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**assignment:** SCD status]

FMT_MSA.4: Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes: [**assignment:** SCD status for new keys is set to "PREACTIVE"].

FMT_SMF.1: Specification of Management Functions

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

- User administrative accounts management (creation, modification, deletion).
- Application accounts management (creation, modification, deletion).
- Key pair generation (SCD/SVD).
- Certificate association SCD activation / deactivation.
- Change of the PIN for activation of the private key.].

FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection:** query] the [**assignment:** audit records] to [**assignment:** administrative users with role Auditor].

FMT_SMR.1/Administrative: Security roles

FMT_SMR.1.1/Administrative: The TSF shall maintain the roles [**assignment:** Administrator, Operator, Security Officers and Auditor].

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

FMT_SMR.1/Applications: Security roles

FMT_SMR.1.1/Applications: The TSF shall maintain the roles [**assignment:** RA, CloudKSP].

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

7.1.7 Class FTA: TOE access

FTA_SSL.3: TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**assignment:** 10 minutes].

FTA_SSL.4: User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

7.2. Dependency analysis for SFRs

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST.

The following table lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

SFR	DEPENDENCIES	SATISFIED
FAU_GEN.1	FPT_STM.1	Justified (1)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCO_NRO.2	FIA_UID.1	FIA_UID.2
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Justified (2) Justified (4)
FCS_COP.1/SAD PIN decipher	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Justified (3) Justified (5)
FCS_COP.1/SAD PIN envelope decipher	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Justified (2) Justified (4)
FCS_COP.1/HMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Justified (2) Justified (4)
FCS_COP.1/SAD signature verification	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1/SSA public key Justified (4)
FCS_COP.2/SCD-SVD generation	No dependencies	N/A
FCS_COP.2/SCD activation	No dependencies	N/A

FCS_COP.2/SAD PIN change	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.6	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.1	No dependencies	N/A
FDP_ACC.1/Administrative	FDP_ACF.1	FDP_ACF.1/Management
FDP_ACC.1/Signer	FDP_ACF.1	FDP_ACF.1/Signature
FDP_ACC.2/Applications	FDP_ACF.1	FDP_ACF.1/Applications
FDP_ACF.1/Management	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 Justified (6)
FDP_ACF.1/Signature	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 Justified (6)
FDP_ACF.1/Applications	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 Justified (6)
FDP_ETC.2/CSR	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1
FDP_ITC.1/Certificate association	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 Justified (6)
FDP_ITC.1/SSA public key	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 Justified (6)
FDP_RIP.1	No dependencies	N/A
FDP_SDI.2	No dependencies	N/A
FDP_SDC.1	No dependencies	N/A
FDP_UDC.1	No dependencies	N/A
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/Signer Justified (7)
FDP_UIT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/Signer Justified (7)
FMT_MSA.1/Accounts	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2/Management FMT_SMR.1/Administrative FMT_SMR.1/Applications FMT_SMF.1

FMT_MSA.1/Create key	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/RA FMT_SMR.1/Applications FMT_SMF.1
FMT_MSA.1/Activate key	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/RA FMT_SMR.1/Applications FMT_SMF.1
FMT_MSA.1/Change SAD PIN	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Signer FMT_SMR.1/Applications FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Create key FMT_MSA.1/Activate key FDP_ACC.1/Signer FMT_SMR.1/Applications
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/Signer
FMT_SMF.1	No dependencies	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1/Administrative FMT_SMR.1/Applications FMT_SMF.1
FMT_SMR.1/Administrative	FIA_UID.1	FIA_UID.2
FMT_SMR.1/Applications	FIA_UID.1	FIA_UID.2
FTA_SSL.3	No dependencies	N/A
FTA_SSL.4	No dependencies	N/A

Table 10 - SFR dependency summary

(1) The dependency with FPT_STM.1 is not fulfilled as the time is obtained by the environment and is not a security functionality provided by the TOE.

(2) The dependency with FCS_CKM.1 is not fulfilled due to the keys are not generated by the TOE. The dependency with FDP_ITC.1, FDP_ITC.2 are not fulfilled due to the keys are loaded from a keystore file by the TOE itself on system startup and not imported through a TSFi.

(3) The dependency with FCS_CKM.1 is not fulfilled due to the keys are not generated by the TOE. The dependency with FDP_ITC.1, FDP_ITC.2 are not fulfilled due to the symmetric keys are generated as a part of SAP protocol in the Signers' SAA and used to encrypt the SAD PIN. The SAD PIN symmetric encryption keys are loaded in memory as part of SAP processing after FCS_COP.1/SAD PIN envelope decipher operation is completed.

(4) The dependency with FCS_CKM.4 is not fulfilled due to the key is not explicitly destroyed by the TOE. The key is kept in memory after being loaded from a keystore and is destroyed when the process is not in memory.

(5) The dependency with FCS_CKM.4 is not fulfilled due to the keys are not explicitly destroyed by the TOE. The keys are kept in memory while the SAD messages are processed as part of the SAP processing and are destroyed when the process is not in memory.

(6) The dependency with FMT_MSA.3 is not fulfilled due the expected initial values set by design of the TOE and cannot be changed. The values can only be modified after creation of the accounts, also for administrative users' or applications' accounts.

(7) The dependencies with FTP_ITC.1 and FTP_TRP.1 are not fulfilled due to the confidentiality, authenticity and integrity of the SAD is achieved by digitally signing the SAD message and encrypting parts of it (the SAD PIN), in consequence a trusted channel or path is not necessary to grant these properties.

7.3. Security Assurance Requirements

The evaluation assurance level is EAL4+ AVA_VAN.5, ALC_FLR.2.

The security assurance requirements are summarized in the following table:

SAR	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_FLR.2** Flaw reporting procedures **ALC_LCD.1** Developer defined life-cycle model **ALC_TAT.1** Well-defined development tools
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.5** Advanced methodical vulnerability analysis

Table 11 - Security assurance requirements

7.4. Rationale for the Security Requirements

7.4.1 Rationale for the Security Functional Requirements

	O.AUTHENTICATION	O.ACCESS_CONTROL	O.SCD_CONFIDENTIALITY	O.SCD_USAGE	O.SCD_SVD	O.SECURE_SIGNATURE	O.DATA_INTEGRITY	O.AUDIT_INTEGRITY	O. KEY_PROT	O. SELFPROTECT
FAU_GEN.1								X		
FAU_GEN.2								X		
FAU_SAR.1								X		
FAU_SAR.2								X		
FAU_SAR.3								X		
FAU_STG.1										X
FAU_STG.4										X
FCO_NRO.2					X					
FCS_CKM.3									X	
FCS_COP.1/SAD PIN decipher				X						
FCS_COP.1/SAD PIN envelope decipher				X						
FCS_COP.1/HMAC					X		X	X		X
FCS_COP.1/SAD signature verification				X		X				
FCS_COP.2/SCD-SVD generation			X	X	X	X				
FCS_COP.2/SCD activation			X	X		X				
FCS_COP.2/SAD PIN change			X	X						
FIA_UID.2	X									
FIA_UAU.2	X									
FIA_UAU.6	X									
FIA_AFL.1				X						
FIA_SOS.1	X									
FDP_ACC.1/Administrative		X								
FDP_ACC.1/Signer		X								
FDP_ACC.2/Applications		X								
FDP_ACF.1/Management		X								
FDP_ACF.1/Signature		X								
FDP_ACF.1/Applications		X								

FDP_ETC.2					X					
FDP_ITC.1/Certificate association					X					
FDP_ITC.1/SSA public key				X						
FDP_RIP.1	X		X	X						
FDP_SDI.2							X	X		X
FDP_SDC.1			X							
FDP_UCT.1			X	X						
FDP_UIT.1						X				
FDP_UDC.1					X					
FMT_MSA.1/Accounts		X								
FMT_MSA.1/Create key		X								
FMT_MSA.1/Activate key		X								
FMT_MSA.1/Change SAD PIN		X								
FMT_MSA.2				X	X					
FMT_MSA.4					X					
FMT_SMF.1				X	X					
FMT_MTD.1		X								
FMT_SMR.1/Administrative		X								
FMT_SMR.1/Applications		X		X	X					
FTA_SSL.3	X									
FTA_SSL.4	X									

Table 12 - Security Functional Requirements rationale

O.AUTHENTICATION

This objective is countered by the identification (FIA_UID.2) and authentication (FIA_UAU.2) of the users accessing to the TOE services.

Administrative users' sessions are protected by allowing the users to terminate their own interactive sessions (FTA_SSL.4) and by automatically closing sessions after an inactivity period (FTA_SSL.3). After session termination users shall re-authenticate to the SSA administrative interfaces (FIA_UAU.6).

Administrative users are authenticated with a password. Passwords shall meet the complexity requirement defined in FIA_SOS.1. Variables with password information are zeroized as soon as the password data is not needed anymore (FDP_RIP.1).

O.ACCESS_CONTROL

Access control policies are defined for accessing to the TOE assets for signature and management (FDP_ACC.1/Administrative, FDP_ACC.2/Applications, ACC.1/Signer, FDP_ACF.1/Management, FDP_ACF.1/Applications, FDP_ACF.1/Signature, FMT_SMR.1/Administrative, FMT_SMR.1/Applications). All the users and applications accessing the TOE services need to have authorization to perform each particular operation.

Also, the security attributes for the particular management operations are defined (FMT_MSA.1/Accounts, FMT_MSA.1/Create key, FMT_MSA.1/Activate Key, FMT_MSA.1/Change SAD PIN). In particular, the access to the audit data is controlled by the appropriate permissions (FMT_MTD.1).

O.SCD_CONFIDENTIALITY

The signature key (SCD) is protected after generation of the HSM (FCS_COP.2/ SCD-SVD generation) and after is stored in the database (FDP_SDC.1) until the activation for its use (FCS_COP.2/SCD activation).

The user's password (SAD PIN) used to encrypt the SCD in combination with the key in HSM can be changed by the owner (FCS_COP.2/Change SAD PIN). The SAD PIN is transmitted encrypted from the SAA to the SSA and can only decrypted by the SSA (FDP_UCT.1). After decryption the password is stored in memory only the time needed and zeroized after use (FDP_RIP.1).

O.SCD_USAGE

The keys for signing are under control of the Signer by the use of a private password (SAD PIN) that is only known by the user that is required to enable the usage of the SDC (FCS_COP.2/SCD activation) having a maximum failure attempts to login (FIA_AFL.1). The SAD PIN protecting and controlling key activation is set at key generation (FCS_COP.2/SCD-SVD generation) and can be changed anytime by the Signer (FCS_COP.2/Change SAD PIN). The SCD can only be activated if the status attribute value is "ACTIVE", when the maximum failure attempts to login are reached the status value is set to "BLOCKED" (FMT_MSA.2).

The SAD is also signed with a private key only in possession of the Signer. The matching public key (SSA public key) is imported into the TOE in the key generation operation (FDP_ITC.1/SSA public key). SAD signature verification (FCS_COP.1/SAD signature verification) is required prior to enable the usage of the SCD acting as the second authentication factor.

The SAD PIN is sent encrypted and can only be deciphered inside the TOE boundaries (FCS_COP.1/SAD PIN decipher, FCS_COP.1/SAD PIN envelope decipher, FDP_UCT.1). After decryption the SAD PIN is stored in memory only the time needed and zeroized after use (FDP_RIP.1).

The generation of the key belongs to the RA functions defined in the TOE (FMT_SMF.1) and can be performed by the authorized applications (FMT_SMR.1/Applications).

O.SCD_SVD

The security measures are established for generating the key pair (FCS_COP.2/SCD-SVD generation) according to the certificate generated (FDP_ETC.2, FCO_NRO.2).

SCD activation and de-activation operations belong to the RA functions defined in the TOE (FMT_SMF.1) and can be performed by the authorized applications (FMT_SMR.1/Applications).

The relationship between the certificate and the keys is established (FDP_ITC.1/Certificate association, FDP_UDC.1) and stored in the database protected by (FCS_COP.1/HMAC verification). New keys are stored with the status attribute set to "PRE-ACTIVE" (FMT_MSA.4), once a certificate is associated to the key pair importing the CA reply the status attribute value is set to "ACTIVE" (FMT_MSA.2).

O.SECURE_SIGNATURE

Keys are generated by the use of strong cryptographic mechanisms (FCS_COP.2/SCD-SVD generation) and the utilization of algorithms for secure signature (FCS_COP.2/SCD activation) through secure channels provided by the operational environment between the TOE and the CloudKSP acting as gateway for the SCA.

DTBSR is protected against modification by digitally signing the SAD message and checking the signature in the TOE (FDP_UIT.1, FCS_COP.1/SAD signature verification).

O.DATA_INTEGRITY

HMAC values are generated for each registry in the database (FCS_COP.1/HMAC).

The TOE includes the verification of the authenticity of the stored data (FDP_SDI.1).

O.AUDIT_INTEGRITY

Audit data are generated by the TOE (FAU_GEN.1, FAU_GEN.2) for storing in the database, and can be accessed (FAU_SAR.1, FAU_SAR.2) by authorized users (FAU_SAR.1).

In addition, HMAC values are generated for each registry in the database (FCS_COP.1/HMAC).

The TOE includes the verification of the authenticity of the stored data (FDP_SDI.1).

The audit integrity will be checked periodically during the TOE execution.

O. KEY_PROT

The keys necessary for the calculation of HMAC values and decipher SAD PIN envelopes are protected (FCS_CKM.3).

O.SELFPROTECT

HMAC values are generated for ensuring the integrity of the data and audit trails stored in the database and allow identifying an unauthorized modification (FCS_COP.1/HMAC).

The TOE includes the verification of the authenticity of the stored data (FDP_SDI.2).

The TOE protects the audit tail against unauthorized deletion (FAU_STG.1) and prevents the lost of audit data events (FAU_STG.4) in case of database unavailability.

Any security violation in the security mechanisms described above triggers a change in the TOE operational state to COMPROMISED preventing the TOE for processing new Signer or RA requests.

7.4.2 Rationale for the Security Assurance Requirements

EAL4 has been selected because it is best suited to addressing the stated security objectives. EAL4 challenges vendors to use best (rather than average) commercial practices and allows evaluating their product at a detailed level, while still benefitting from the Common Criteria Recognition Agreement.

The AVA_VAN.5 augmentation has been added to provide assurance that the TOE will be highly resistant to penetration attacks to meet the security objectives O.SCD_CONFIDENTIALITY, O. SCD_USAGE and O.SECURE_SIGNATURE.

The ALC_FLR.2 augmentation has been added to provide assurance that the TOE will be maintained and supported in the future, requiring that discovered security flaws will be tracked and corrected by the developer.

The chosen assurance level is appropriate for the threats defined in the environment.

8. TOE summary specification

8.1. System management

The TOE support roles with different privileges.

The TOE support the following roles associated to TOE management operations (FMT_SMR.1/Administrative, FMT_SMF.1). These roles are referred as administrative or privileged roles:

- Security Officer (SO): having the overall responsibility for administering the implementation of the security policy, including the application and administrative user management (FMT_MSA.1/Accounts).
- System Administrator (ADM): is authorized to install and configure the TOE.
- System Operator (OP): is authorized to perform system start-up, shutdown, backup and recovery.
- System Auditor (AU): are authorized to view audit logs. (FMT_MTD.1)

Users are assigned to roles. Users assigned to role Auditor or Operator are not able to configure or administer the TOE. The TOE enforces separation of duties based on the following rules:

- A user assuming the AU role is not authorized to assume SO, ADM or OP roles.
- A user assuming the SO role is not authorized to assume AU, ADM or OP roles.

The TOE supports the following roles associated to the signature generation services operations (FMT_SMR.1/Applications, FMT_SMF.1). These roles are referred as un-privileged roles:

- RA: application authorized to request signer key pair (SCD/SVD) generation on behalf of the Signer and certificate association SCD activation / deactivation (FMT_MSA.1/Create Key, FMT_MSA.1/Activate Key).
- CloudKSP: applications authorized to send DTBS requests and SAD PIN change requests on behalf of the user.

The CloudKSP application acts as a reverse proxy forwarding the DTBS requests from the SCA and the SAD from the Signer's SAA to the TOE. Signers are granted with the role CloudKSP in the TOE, which enables the Signer to authorize the use his SCD and to change his SAD PIN used in the SAP to activate his SCD (FMT_MSA.1/Change SAD PIN).

8.2. Identification and authentication

The TOE requires each user (privileged or un-privileged) to be successfully identified and authenticated before allowing any operation (FIA_UID.2, FIA_UAU.2).

Administrative operations are only available through the TOE administrative TSFi and cannot be invoked remotely. Administrative operations interface requires users to identify and authenticate with username and password. The TOE enforces that Administrative

users' password meet the complexity requirements defined in the password policy (FIA_SOS.1).

Once the user is authenticated an interactive session is established and the user does not need to re-authenticate until he is logged-out (FIA_UAU.6). Administrative users are able to terminate their interactive sessions (FTA_SSL.4) by calling the logout TSFi. The unattended interactive sessions are closed after 10 minutes of inactivity (FTA_SSL.3).

Signature generation services operations can be invoked remotely and require the invoking applications to identify and authenticate with a digital certificate.

The signer is authorized to use is SCD after successfully authenticate with his SAD PIN, if three unsuccessful authentication attempts occur the signer's SCD is blocked (FIA_AFL.1).

8.3. Access control

Access control to the TOE is based on the concept of TOE users associated to roles. Each of the defined roles is configured with a set of permissions and/or restrictions about the operations and objects that it can (or cannot) access (FDP_ACC.1/Administrative, FDP_ACC.2/Applications, FDP_ACF.1/Management, FDP_ACF.1/Applications).

Signer access control policy to his SCD is defined in (FDP_ACC.1/Signer) and the access rules to be fulfilled in each operation over the SCD are defined in (FDP_ACC.1/Signature). In order to perform any operation over his SCD the Signer shall send the SAD.

8.4. Key management and cryptographic operations

Keys managed by the TOE are separated in three categories:

- Signer's signing keys
- Signer's SAD keys
- Infrastructure keys: keys used by the TOE for processes like configuration and audit log signing, message authentication and session keys.

Signer's signing keys are generated in a HSM evaluated and certified Common Criteria EAL4+AVA_VAN.5. The signer's private key (SCD) is wrapped with a symmetric key and exported from the HSM. To grant singer's sole control over the private key a wrapping key is derived from the user's SAD PIN and a master key in the HSM (FCS_COP.2/SCD-SVD generation, FDP_SDC.1.1). Signer's encrypted SCD is stored in a database. In the Signer's key pair generation request the Signer's SSA public key needed to verify the SAD messages is imported into the SSA (FDP_ITC.1/SSA public key). The Signer's key pair generation process creates a PKCS#10 certificate request signed with the Signer's private key. The PKCS#10 is returned to the RA in response to the create key pair operation and is used by the RA in order to check that the Signer is in possession of the private key (FCO_NRO.2, FDP_ETC.2) in the process of issuing a qualified electronic certificate binding the Signer's identity with his public key.

The Signer's SCD is not usable until it is activated by the RA (SCD status on generation is set to "PRE-ACTIVE" (FMT_MSA.4)). In the activation operation the RA sends to the TOE the

electronic certificate for the Signer's public key. The TOE checks the correspondence between the electronic certificate and the Signers SVD (FDP_ITC.1/Certificate association) and if this operation ends with success the SCD is marked as usable (SCD status is set to "ACTIVE" (FMT_MSA.2)) and its security attributes are updated with the expiration date read from the electronic certificate. The TOE enforces that the Signer is not able to use his key after his certificate is expired.

The Signer's SCD can only be loaded and used to perform cryptographic operations inside the HSM boundaries if its status value is "ACTIVE" (FMT_MSA.2) and after the SAD is verified and the Signer is authenticated (FCS_COP.1/SAD signature verification, FCS_COP2/SCD activation). It the Signer's reaches the maximum failure attempts for entering the SAD PIN the SCD status value is set to "BLOCKED" (FMT_MSA.2),The TOE invokes the operation FCS_COP.2/SAD PIN change for changing the SAD PIN used to protect his private key. This operation requires the activation of the SCD in the HSM with the old SAD PIN, creation of a new wrapping key from the combination of the new SAD PIN and the HSM master key and wrapping the SCD with it.

Signer's SAD keys are generated in Signer's local environment using his SAA. SAD PIN encryption key is transmitted to TOE in the SAD message encrypted with a public key. The TOE recovers the SAD PIN encryption key and deciphers the SAD PIN executing FCS_COP.1/SAD PIN envelope decipher and FCS_COP.1/SAD PIN decipher.

Infrastructure keys are generated outside the TOE and stored in a password protected encrypted Java KeyStore (JKS) (FCS_CKM.3). Infrastructure keys are loaded from the TOE's KeyStore and used for several purposes:

- Grant configuration data integrity and authenticity by computing HMAC (FCS_COP.1/HMAC) of the records stored in the database.
- Grant audit log trail integrity and authenticity by computing HMAC (FCS_COP.1/HMAC) of each audit entry and the full trail.
- Decipher SAD PIN envelopes as part of the SAP (FCS_COP.1/SAD PIN).

8.5. SAD/SAP protection

The SAD message is transmitted from the Signer's SAA to the SSA as part of the SAP. The SAD message integrity and authenticity is granted by the use of a digital signature over the SAD message (FDP_UIT.1) done with a private key which corresponding public key is registered in the TOE when the Signer's SCD/SVD is created. DTBSR is included as a part of the SAD, so its integrity and authenticity is granted by the same mechanism.

The SAD PIN is also transmitted in the SAD. In order to prevent SAD PIN from disclosure it is ciphered in the Signer's SAA and can only be recovered by the TOE (FDP_UCT.1) (see section 2.4.2 for more details).

8.6. Residual information protection

Variables containing sensitive information like the Administrative user's passwords and unencrypted SAD PINs are zeroized as soon as the data in not needed anymore (FDP_RIP.1).

8.7. Audit

The TOE generates audit records for all the events listed in Table 9 (FAU_GEN.1, FAU_GEN.2). Audit logs are stored in the database and can be exported and reviewed at request of an Auditor (FAU_SAR.1). The TOE protects each individual audit record stored in the database computing its HMAC value. Each audit record is chained to the previous entry in the audit log, allowing the TOE to detect unauthorized deletions (FAU_STG.1). The TOE stops processing new requests from the RA and Signer interfaces if the audit trail is not available for new insertions (FAU_STG.4).

Auditor is the unique administrative role with read access to the audit trail (FAU_SAR.2). The TOE provides the users assigned with the Auditor role with an interface for selecting sets of audit records based on search criteria like date and time, type of event, operation result (success or failure) and generator entity (FAU_SAR.3).

8.8. Database data protection

Signer's data, TOE configuration data and the audit trail are stored in a database hosted outside the TOE. The TOE protects each record stored in the database with its HMAC value. Each time a record is read from the database, the TOE checks the HMAC value is correct, assuring the integrity and authenticity of the data and stops processing new requests from the RA and Signer interfaces if HMAC check fails (FDP_SDI.2). Moreover, the audit integrity will be checked periodically during the TOE execution.

8.9. Secure communications

Communication between client applications and the TSF is always secure using the TLS protocol. TLS channels are provided and configured in the JBOSS server as a part of the operational environment. No un-secured communication from external applications is allowed.

9. Terminology

Administrative user: a TOE user role that performs management functions over the TOE by accessing the command line client.

Advanced electronic signature: an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;
b) it is capable of identifying the signatory;
c) it is created using means that the signatory can maintain under his sole control, and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data: information used to verify the claimed identity of a user.

Certificate: an electronic attestation which links the SVD to a person and confirms the identity of that person.

Certification service provider (CSP): means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Data to be signed (DTBS): the complete electronic data to be signed, such as QC content data or certificate status information.

Data to be signed representation (DTBSR): the data sent to the TOE for signing and that is a hash-value of the DTBS.

Digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2]

Hardware security module (HSM): means the cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE.

Qualified certificate: a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a CSP who fulfills the requirements laid down in Annex II of the Directive.

Signature creation application (SCA): application that creates a signed document, using the digital signature produced by the SSA.

Signature authentication application (SAA): piece of software operated in the Signer's environment under his sole control used in the SAD generation process of the SAP.

Signature activation data (SAD): secret belonging the signer that needs to be provided to the SCD for enabling the key in the SCD for its use.

Signature activation protocol (SAP): protocol that collects the SAD used to control a signature operation on a DTBSR using the signing key of the Signer.

Signature creation device (SCD): configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive.

Signature-creation data (SCD): unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature-verification data (SVD): data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Signer: entity (human or external IT entity) outside the TOE that interacts with the TOE for requesting signature services.

Verification authentication data (VAD): authentication data provided as input by knowledge or authentication

10. References

[CEM]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 3.1 Revision 5
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1, 2 and 3 Version 3.1, Revision 5
[CEN]	CEN/TS 419 241 Security Requirements for Trustworthy Systems Supporting Server Signing
[eIDAS]	Regulation 910/2014/EU of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[ESI312]	ETSI TS 119 312 Electronic Signature and Infrastructures (ESI); Cryptographic Suites for Electronic Signatures
[SOGCRYPT]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.0
[ESI401]	EN 319 401-1 Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.