SECURITY TARGET FOR

SIMPLYSIGN SIGNATURE ACTIVATION MODULE (SAM)

Common Criteria version 3.1 revision 5

Assurance Level EAL 4+

Version 1.25 LITE

Table of Contents

Terms

AT	Access Token
CA	Certification Authority
CAS	Central of Authentication Service
CKS	Cloud Key Service
CM	Cryptographic Module
CSR	Certification Signing Request
DTBS/R	Data To Be Signed Representation
HSM	Hardware Security Module
IDP	Identity Provider
PIN	Personal Identification Number
QSCD	Qualified Electronic Signature Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SCAL	Sole Control Assurance Level
SCD	Signature and Seal Creation Data
SCDev	Signature Creation Device
SCS	SoftCard System
SCKS	SimplySign Cloud Key Service
SIC	Signer Interaction Component
SSA	Server Signing Application
SVD	Signature Verification Data
TOTP	Time-based One Time Password
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing

TVP	Time Variant Parameter
UTC	Coordinated Universal Time

1. Introduction

1.1. ST Overview

This ST document defines the security objectives and requirements as well as the scope of the evaluation of the common criteria for SimplySign SAM - Signature Activation Module.

The Target of the Evaluation (TOE) is the SimplySign SAM software that handles user registration and signing requests through user's Signature Application (SCA) that exploits Signer Interaction Component (SIC).

TOE is supported by the following software platform to accomplish its tasks:

- SimplySign SSA: which acts between SCA (with SIC) and the TOE (SimplySign SAM);

and it includes the following non-software components:

- *SimplySign SAM Preparative guidance*,
- *SimplySign SAM Operational guidance*.

To ensure a secure execution environment, the TOE is delivered in a tamper-protected form (TOE and documentation are placed as TOE archive whose integrity is protected by a checksum computed as a SHA256 or SHA512 hash value) to provide a secure execution environment.

TOE provides a remote Qualified Electronic Signatures and Seals (QES) service according to eIDAS Regulation 910/2014 [1] at the SCAL2 (Sole Control Assurance Level 2) level according to EN 419 241-1 [2].

1.2. ST Reference

This ST is identified by the following unique reference:

ST Title	Security Target for SimplySign Signature Activation Module (SAM)
ST Version	V_1.25 LITE
ST Date	2024-02-01
ST Author	Asseco Data Systems

Note from ST Author: this is lite version of the original ST document that is referenced by its ST Version: V_1.25, without "LITE" appended.

1.3. TOE Reference

The TOE is identified by the following unique reference:

TOE Name	SimplySign Signature Activation Module (SAM)
TOE Version	6.2.0
Evaluation Criteria	Common Criteria version 3.1, revision 5, April 2017 Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, version 3.1, revision 5, April 2017.
Evaluation Assurance Level	EAL 4 augmented by AVA_VAN.5
TOE Developer	Asseco Data Systems
TOE Sponsor	Asseco Data Systems
Evaluation Facility	ITSEF NIT, Poland
Certification Authority	NASK National Research Institute, The Center for Standardization and Certification, Poland
Certification ID	[2021-4]

1.4. TOE Overview

SimplySign is a TW4S system (Trustworthy System Supporting Server Signing) that offers a remote digital signature as a service. TOE (SimplySign SAM) ensures that Signer's signing key or keys are only used under the sole control of the Signer for the intended purpose.

The SimplySign system consists of local (a Signer with a Signing Application) and remote environment, using an EN 419 221-5 compliant Cryptographic Module (CM) [3] to generate the signing key and create the digital signature value (Figure 1). The Signer is in the local environment and interacts with the Signing Application (that includes Signer Interaction Component - SIC) which communicates with the SimplySign SSA (Server Signing Application) in the remote environment to use the signing service. The signature operation is performed using the Signature Activation Protocol (SAP), which requires Signature Activation Data (SAD) be provided at the local environment, and next transfers SAD to the remote environment.

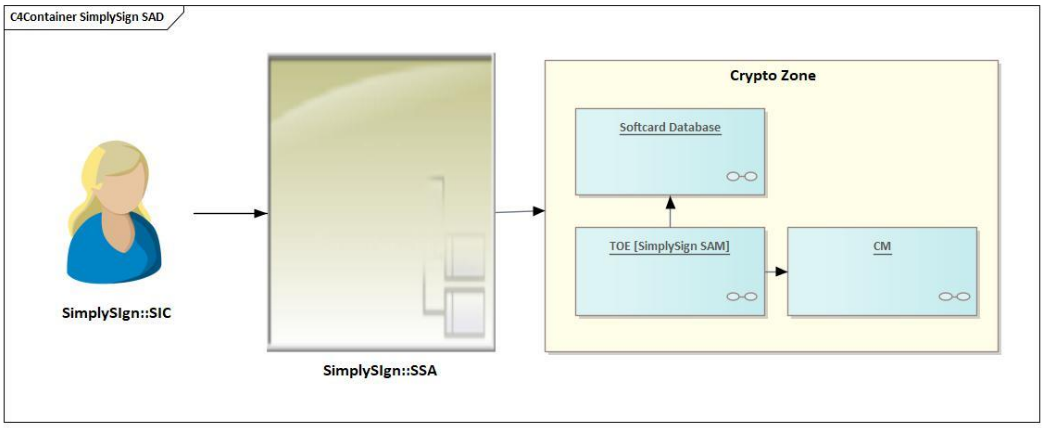


Figure 1: SimplySign System

SimplySign SAM (TOE) is a software component that operates in a dedicated tamper-protected environment called CryptoZone.

Signer is a person who has the signing key under his/her sole control after being connected to the SimplySign system. It is recognized in the SimplySign system as a card (electronic form) with unique card number.

The TOE along with the CM (the CM is provided as a module embedded in the CryptoZone and connected to the TOE through a trusted channel) provides the necessary functionality to protect the Signer attributes needed to generate a digital signature. Other components (external components needed by the Signer to interact with the TOE, as presented in Figure 2) are parts of the SimplySign SSA environment.

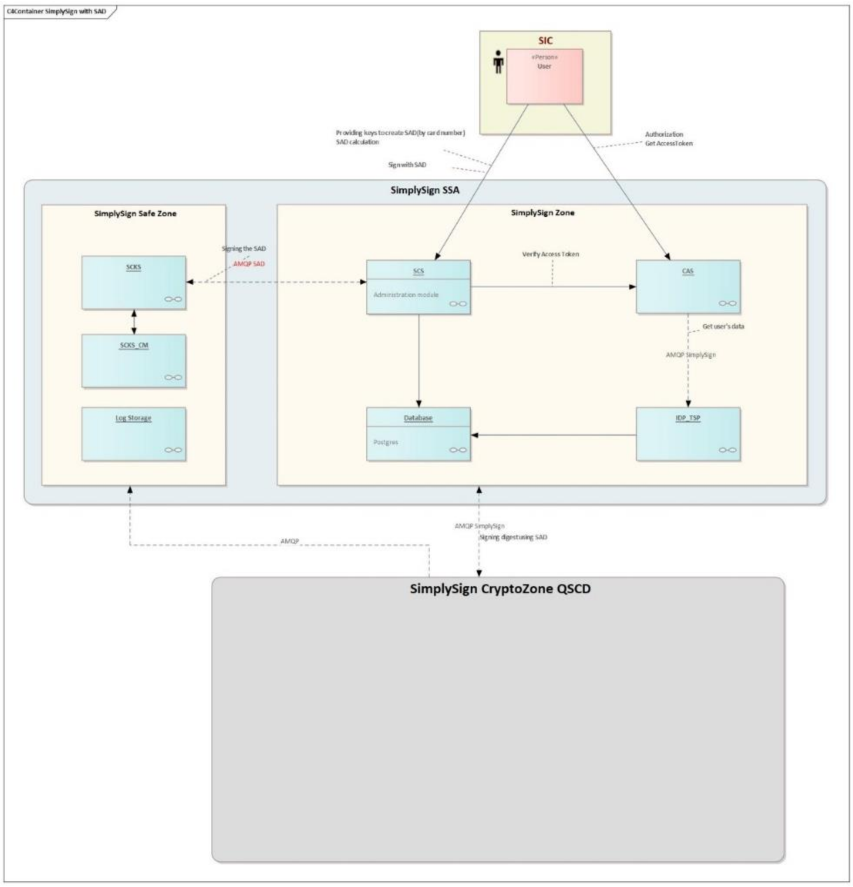


Figure 2: Required non-TOE Components

Signing process is initiated by Signer by preparing SAD. The SAD consists of:

- The cryptogram obtained by encrypting, with the TOE public key.
- Signer AT token,
- certificate of the Signer public key,
- signature algorithm identifier,
- TOE public key identifier,
- hash algorithm identifier,
- card number that indicates where the Signer's cryptographic data (SCD) are located.

Thus prepared SAD together with DTBS/R(s) is sent to the SCS module (an element of SimplySign SSA).

SCS module performs the following processes:

- first checks the compliance of the length of the cryptogram and the TOE public key (a non-compliance causes the protocol to be aborted and an error is signalled);
- then sends the AT token obtained from the SAD to the CAS (an element of SimplySign SSA) for verification and obtaining information about the UUID of the Signer associated with this token;
- after receiving a positive response from CAS, SCS checks in the Database module of SimplySign SSA whether the certificate placed in the SAD associated with the UUID of the Signer obtained from CAS exists and is valid;
- a positive result authorizes the SCS module to communicate with the SCKS module of SimplySign SSA to sign the SAD using the SimplySign SSA private key.

- The signed SAD along with the DTBS/R(s) is securely transmitted (AMQP protocol supported by TLS) to the TOE (SimplySign SAM) module.

For the Signers to have exclusive control over their signing keys, the signing operation must be authorized. Authorization is performed by the TOE by activating the signing key within the CM, after prior verification of the SAD. Verification of the SAD means that the TOE checks the complementarity between all elements of the SAD (cryptogram, AT token, card number, Signer's public key certificate, TOE public key identifier, signature algorithm identifier, hash algorithm identifier), as well as it verifies whether the Signer is authenticated (by verifying Singer's PIN and the SimplySign SSA signature).

The verification of the SAD is performed by the TOE in the following order (checking the links between different objects):

- Decryption of the cryptogram with the TOE private key indicated (by the TOE public key identifier) in the SAD. The result of the decryption is information about the cryptogram hash.
- Checking the compliance of the cryptogram hash with the hash calculated for the concatenation of the following data (to ensure the integrity of the SAD, the Signer's PIN and the UTC time when the SAD was created)

  If the hashes are not compliant, the protocol is aborted (lack of SAD integrity).

- Checking the actual time/freshness of the SAD by comparing the UTC time retrieved from the cryptogram for the SAD with the current UTC time in the TOE. If the tolerated delay in protocol execution is exceeded, the protocol is aborted.
- Searching, by referring to the card number, in the SoftCard Database for data corresponding to the signing key indicated indirectly (by a public key) in the Signer certificate. Checking the correctness of the stored PIN against the PIN obtained from the SAD. If the PIN is correct, it successfully completes the SAP protocol and the signing of the DTBS/R(s) is performed.
- Signed DTBS/R(s) are sent back to the remote signer via the SimplySign SSA.

Signer authentication in the TOE is accomplished as a combination of the following:

- Direct authentication, based on PIN, and,
- Indirect authentication, when the TOE verifies the assertion created in SCS module.

All Signer interactions with the TOE (SimplySign SAM) through the component SIC is conducted by the SimplySign SSA service. TOE communicates with the SimplySign SSA to obtain the signature request. Once the TOE has verified the SAD, it can authorize the activation of the signing key within the CM and creates a digital signature value. The value is returned to the SimplySign SSA and may be further delivered to the Signing Application (SCA). The TOE generates audit records for all security related events and relies on the SimplySign SSA (Log Storage component) to store and provide access control for the records.

Signature and Seal Creation Data (SCD) is encrypted by the CM and stored outside the CM, in the SoftCard Database. When SCD is active and after successful Signer authentication, SCD is uploaded to the CM before signature or seal generation. All SCD operations (generation, usage, destruction) are implemented using certified secure methods provided by the CM.

1.4.1. TOE Type

TOE (SimplySign SAM) is a software component. TOE together with a CM certified against EN 419221-5 [3] constitutes a QSCD. The TOE along with the CM operates in a dedicated hardware appliance called CryptoZone, which resides in tamper-protected environment. The TOE is connected to the CM via trusted channel.

The TOE implements the Signature Activation Protocol (SAP). The TOE uses Signature Activation Data (SAD) from the Signer to activate the corresponding signing key within CM.

1.4.2. TOE Usage & Major Security Features

TOE (SimplySign SAM) ensures that the remote signer has sole control of his signing keys according to EN 419241-1 [2]. This means that the signing operation must be authorized using the signing application (SCA) with SIC.

The Signer, using the Signature Creation Application (SCA) with SIC, communicates via SimplySign SSA with the TOE to submit the SAD. The SAD binds together the Signer's authentication with the signing key and the data to be signed representation DTBS/R(s). During remote signing operations, all communication between the Signer and the TOE is performed through the SimplySign SSA.

The main security features of the TOE are:

- Identification and authentication of TOE users;
- Secure creation and management of TOE users;
- Signer key pair generation and deletion;
- Suppling DTBS/R;
- Remote signing;
- Audit of all security relevant events;
- Secure communication between TOE and SimplySign SSA.

1.4.3. Required non-TOE Hardware/Software/Firmware

The following hardware/software/firmware is required to operate the TOE (SimplySign SAM), which are excluded from the TOE (see Figure 2):

- SCA with SIC that prepares DTBS/R(s), logs the user into the system, prepares the SAD, sends (using SIC) the SAD along with the DTBS/Rs to the SCS module, finally creates (formats) signed document based on the signed DTBS/R(s).
- SimplySign SSA, which acts between the SCA (with SIC) and the TOE (SimplySign SAM) located in the CryptoZone (QSCD).

TOE needs to be run using so called CryptoZone: a dedicated hardware appliance that operates in tamper-protected environment in accordance with the requirements of EN 419241-1 [2]. Except TOE, CryptoZone shall include the following CM (Cryptographic Module): nCipher nShield Solo XC product family provided by Entrust, and certified in accordance with EN 419 221-5 [3]; the CM performs cryptographic operations invoked by the TOE (SimplySign SAM). Moreover, CryptoZone hardware appliance keeps SoftCard Database where TOE related data is securely stored. The database occurs in the form of encrypted files or as a Postgres SQL database, depending on one of the two TOE modes of operation: PKCS or CT (CipherTools), respectively.

The hardware appliance CryptoZone needs to meet the following hardware and software requirements:

- at least 2 CPU: Intel or AMD CPU models that meets CPU requirements of used operating system,
- minimum: 4GB RAM, 10 GB HDD/SDD,
- operating system: RedHat 7 (or higher), with the following packages: PostgreSQL Database Server (version 12 or higher), PGBouncer and rsync.

The above mentioned components enable the implementation of a remote signature service according to eIDAS Regulation 910/2014[1] at SCAL2 level according to EN 419 241-1 [2].

1.5. TOE Description

TOE (SimplySign SAM) allows authenticated users (Signers) to create digital signatures. With secure protocols, physical and logistical security policies for the TOE operational environment, and strict administrative procedures, a remote electronic signature service can be provided to signers.

TOE (SimplySign SAM) is a software component that provides remote signature/seal creation (signing DTBS/R(s)). The TOE together with the CM (the CM is a module installed in the CryptoZone and connected to the TOE through a trusted channel) constitute a QSCD (Qualified Electronic Signature Creation Device) according to EN 419241-1 [2]. The TOE is located in a tamper-protected environment (dedicated hardware appliance – CryptoZone). It is constructed in such a way that it is responsible for the executed operation logic according to the requirements of EN 419241-2 [4].

TOE is supported by:

- SimplySign SSA: it provides various services including Signer account registration, Signer key registration, log saving and archiving, etc.
- SCA with SIC: it manages the document to be signed and transfers it to the SSA.

1.5.1. Physical Scope of the TOE

The TOE is a SAM software component that operates in dedicated hardware appliance. The appliance constitutes tamper-protected environment called CryptoZone. TOE is connected to the CM (embedded in the hardware appliance) through a trusted channel. The CM is installed with its software that provides the CM API.

The physical boundary of the TOE shall be tamper-protected in accordance with the requirements of EN 419241-1 [2].

The TOE operates in two configurations: PKCS or CT, depending on which API (library) of the CM module is used (PKCS#11 or CipherTools, respectively). Both configurations (PKCS and CT) represent TOE evaluated configurations.

TOE consists of the following components:

1) Main TOE application called CKS;
2) Additional libraries and configuration files for PKCS and CT configurations.

that are supplemented by guidance documentation: *SimplySign SAM Preparative guidance* and *SimplySign SAM Operational guidance.*

Moreover, the following supporting package is provided together with the TOE (the package is not a TOE component):

TOE supporting tools that are used for export/import cryptographic keys

1.5.1.1. Delivery of the TOE

The TOE (SimplySign SAM) is delivered in a tamper-protected TOE archive file: *CKS_v6.2.0.0.zip*.

The TOE, along with the associated documentation (*SimplySign SAM Preparative guidance* and *SimplySign SAM Operational guidance*) is placed in Artifactory repository system as a single archive file (ZIP file or TAR file – according to client requirements). TOE delivery is accomplished by emailing to a client a link to the archive file and a checksum calculated as the SHA256 or SHA512 hash value of the TOE archive file.

TOE main archive file *CKS_v6.2.0.0.zip* includes the following components presented in the table below.

No	Type	Description	Name of the archive/file
1.	Software	Main TOE application called *CKS*	CKS_v6.2.0.0.zip
2.	*Software*	*TOE supporting tools (non-TOE component)*	*toeTools-1.0.0.zip*
3.	Documentation	Preparative guidance	AGD_PRE EAL4 for SimplySign SAM v.0.95.pdf
4.	Documentation	Operational guidance	AGD_OPE EAL4 for SimplySign SAM v.0.94.pdf

1.5.2. Logical Scope of the TOE

The TOE (SimplySign SAM) provides a system for creating digital signatures as required by the eIDAS regulation. This chapter describes the logical security features offered by the TOE.

1.5.2.1. Roles & Available Functions

The TOE maintains the following roles: Privileged User and Unprivileged User – a Signer:

a) **Privileged User** - there is only one Privileged User in SimplySign SAM, which is SimplySign SSA. It executes various TOE specific operations, e.g., creates and manages Signers.
b) **Signers** - can request remote signing operations by interacting with SimplySign SSA and next authorizes these operations using the Signature Creation Application (SCA) to provide the required authentication data and SAD.

To activate a signing key in the TOE, the Signer had to be authenticated using SimplySign SSA (delegated authentication). The SAD is also required to activate Signer's signing key, because one of the SAD elements is a PIN code provided by the Signer in the SCA and next verified by the TOE (direct authentication).

Privileged User is created and authenticated during TOE initialization, by TLS certificate.

Privileged User and Signers can generate signing keys and Signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a Signer, as well as can disable a signing key identifier to be used by a Signer.

Moreover, the role of System Administrator is considered. System Administrator configures the TOE by editing the configuration files, and administrates TOE application from the level of operating system account (start/stop TOE application, checking the status of TOE service etc.). This role is not implemented as a TOE functionality. System Administrator is authenticated at the operating system level, using operating system accounts.

1.5.2.2. Signature operation

The TOE allows Signers to carry out remote signature. For signing operations, the TOE offers the following features:

- Signer can provide DTBS/R(s) for signing.
- The link between the Signer's authentication data, DTBS/R(s) and the Signer's key identifier is provided by the Signature Activation Data (SAD). The SAD is securely exchanged with the TOE using Signature Activation Protocol (SAP). Within the TOE, the following actions are performed:
  - the TOE receives Signer's authorization request, with SAD and DTBS/R(s),
  - the TOE verifies delegated authentication assertion and SADs provided by the Signer, and checks if the SAD binds together the Signer authentication, a DTBS/R(s) and signing key identifier,
  - based on signing key identifier assigned to the Signer, the TOE activates the signing key within CM using Signer's Authorization Data,
  - the TOE uses CM to create signature.

UTC time is the component of the SAD. This time is verified in the TOE (SimplySign SAM) after the SAD has been decrypted. It is assumed that "not too much" time can elapse between the creation of the SAD and its verification. Additionally, the TOE remembers its last value for a given Signer's AT and rejects repetitions. This way, TOE defends itself against a replay attack.

1.5.2.3. Audit

All events related to TOE security and Signers are recorded. SimplySign SSA provides access to logs intended for security auditing.

The event log covers all security relevant events. Each record is protected to prevent modifications, records are chained to prevent deletion. All audit records created by actions of Privileged User, and those created by requests handled by the TOE, are stored in the Log Storage component of SimplySign SSA. The connection between the TOE and Log Storage Component is provided using AMQP protocol secured with TLS. The audit trail does not include any data which allow to retrieve sensitive information.

1.5.2.4. Trusted Communication

TOE implements and enforces the following trusted communication methods and protocols:

- CM: the TOE (SimplySign SAM) communicates with the CM, located in the same hardware appliance, by direct calls of CM's vendor specific APIs. The API requires the TOE to transmit to the CM: a user card reference, a user PIN, a user private key reference. Upon successful verification of the PIN, the CM activates the user's private key and enables the signing of DTBS/R(s). Communication with the CM is only possible through the provided API of the CM vendor (the CM is part of QSCD, certified to meet the requirements of EN 419 221-5 [3]).
- SimplySign SSA: communicates with the TOE (SimplySign SAM) by exchanging AMQP protocol messages that are transferred through TLS channel established between the SSA and the TOE.
- Signature Creation Application: The Signature Creation Application (SCA) connects indirectly to the TOE, via SimplySign SSA, using an authenticated TLS channel between SimplySign SSA and the TOE.

1.5.3 TOE life Cycle

The TOE life cycle consists of the following phases: development, delivery, installation and configuration, operational use:

- Development phase: the TOE developer develops the TOE (SimplySign SAM) application and its guidance documentation using any appropriate guidance documentation for components working with the TOE, including the CM.
- Delivery phase: the TOE is securely delivered from the TOE developer to a Customer – TOE operator.
- Installation and Configuration phase: TOE operator installs and configures the TOE with the appropriate configuration and initialization data, what includes creation of TOE Privileged User.
- Operational phase: The TOE is managed by SimplySign SSA (the Privileged User) who can create Signers. Privileged Users and Signers may generate signature keys for a Signer. Signers can supply the data to be signed to the TOE, along with Signature Authorization Data. Only Signers can authorize signature creation.

2. Conformance Claims

2.1. CC Conformance Claim

This security target is written according to Common Criteria version 3.1 revision 5 [6], [7], [8].

More precisely, this security target claims to be:

- Common Criteria Part 2 [7] extended;
- Common Criteria Part 3 [8] conformant.

The assurance requirement of this security target is **EAL4 augmented**. Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis

2.2. PP Conformance Claim

This security target claims strict conformance to the following protection profile:

- EN 419 241-2 [4]: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing, February 2019.

2.3. Conformance Rationale

This security target claims strict conformance to the EN 419 241-2 [4] Protection Profile.

The TOE and associated Cryptographic Module are a QSCD, as described in [4].

The Security Problem Definition (Section 3) of this ST includes the assets, the subjects, the assumptions, the threats and the organizational security policies as defined in the PP [4].

The Security Objectives (Section 4) of this ST includes the security objectives as defined in the PP [4].

The Security Functional Requirements section (6.4) of this ST include all SFRs presented in the PP [4]. Iterations and changes to the SFRs introduced in this ST, with respect to the PP [4], do not lower TOE security.

The Security Assurance Requirements section (6.5) of this ST claims conformance to EAL4 augmented with AVA_VAN.5. This is the package of security assurance requirement allowed for conformance to the PP [4].

3. Security Problem Definition

3.1. Assets

The TOE has the following assets, which are to be protected in integrity and confidentiality as described below. The TOE must ensure that whenever an asset is persisted outside the TOE, the TOE has performed the necessary cryptographic operations to enforce confidentiality and detect if an asset has been modified. Access control to TOE assets outside the TOE are to be enforced by the environment.

R.Signing_Key_Id: The signing key is the private key of an asymmetric key pair used to create a digital signature under the Signer's sole control. The signing key can only be used by the CM. The TOE uses the asset R.Signing_Key_Id, which identifies a signing key in the CM. The binding of the R.Signing_Key_Id with R.Signer shall be protected in integrity.

Application Note 1 (Application Note 1 from [4], refined by ST author)

The integrity and confidentiality of the signing key and the link between the R.Signing_Key_Id and the signing key is the responsibility of the CM

R.Authorisation_Data: is data used by the TOE to activate a signing key in the CM. The signing key is identified by R.Signing_Key_Id. It shall be protected in integrity and confidentiality.

Application Note 2 (Application Note 2 from [4], refined by ST author)

The R.Authorisation_Data are used by the CM to activate a signing key.

R.Authorization_Data2: is data used by the TOE to change and reset R.Authorization_Data.

R.SVD: signature verification data is the public part, associated with the signing key, to perform digital signature verification. The R.SVD shall be protected in integrity.

The TOE uses a CM for signing key pair generation. As part of the signing key pair generation, CM provides the TOE with R.Signing_Key_Id and R.SVD. The TOE provides the R.SVD to the SSA for further handling for the key pair to be certified.

Application Note 3 (from ST author)

The integrity of the R.SVD is guaranteed by the CM (compliant with EN 419 221-5 [3]).

R.DTBS/R: set of data which is transmitted to the TOE for digital signature creation on behalf of the Signer. The DTBS/R is transmitted to the TOE. The R.DTBS/R shall be protected in integrity.

Application Note 4 (Application Note 3 from [4])

The confidentiality of the R.DTBS/R is not required by Regulation (EU) No 910/2014 eIDAS [1].

R.SAD: SAD is a set of data involved in the SAP, which activates the signature creation data to create a digital signature under the Signer's sole control. The R.SAD shall combine:

- The Signer's strong authentication as specified in EN 419 241-1 [2].
- If a particular key is not implied (e.g. a default or one-time key) a unique reference to R.Signing_Key_Id.
- A given R.DTBS/R.

The R.SAD shall be protected in integrity and confidentiality.

Application Note 5 (Application Note 4 from [4], refined by ST author)

The SAD contains confidential authentication data (PIN) for activating the user's private key in the CM.

Application Note 6 (Application Note 5 from [4])

The R.SAD may include some or all authentication factors or evidence from other systems that some or all authentication factors have been verified.

Application Note 7 (Application Note 6 from [4], refined by ST author)

The unique reference to R.Signing_Key_Id in R.SAD is the derived information obtained from the signer's authentication

R.Signature: is the result of the signature operation and is a digital signature value. R.Signature is created on the R.DTBS/R using R.Signing_Key_Id by the CM under the Signer's control as part of the SAP. The R.Signature shall be protected in integrity. The R.Signature can be verified outside TOE using R.SVD.

R.Audit: is audit records containing logs of events requiring to be audited. The logs are produced by the TOE and stored externally. The R.Audit shall be protected in integrity.

R.Signer: is a TOE subject containing the set of data that uniquely identifies the Signer within the TOE. The R.Signer shall be protected in integrity and confidentiality.

Application Note 8 (Application Note 7 from [4], refined by ST author)

It is only within the TOE the R.Signer needs to be unique. It is not the responsibility of the TOE to establish a connection between the R.Signer and the signer's identity. The Signer is said to own the R.Signer object which uniquely identifies him within the TOE.

Application Note 9 (Application Note 8 from [4])

The R.Signer can include references to zero, one or several R.Signing_Key_Ids and R.SVDs.

Application Note 10 (Application Note 9 from [4], refined by ST author)

R.Reference_Signer_Authentication_Data: is the set of data used by TOE to authenticate the Signer.

The R.Reference_Signer_Authentication_Data shall be protected in integrity and confidentiality.

Application Note 11 (Application Note 10 from [4], refined by ST author)

The R.Reference_Signer_Authentication_Data is used by the TOE to authenticate the Signer, and the R.Authorisation_Data is used by the TOE to activate a signing key in the CM.

Application Note 12 (Application Note 11 from [4], refined by ST author)

Reference_Signer_Authentication_Data contains a PIN in encrypted form, and the SVD for assertion verification in nonconfidential form.

R.TSF_DATA: is the set of TOE configuration data used to operate the TOE. It shall be protected in integrity.

Application Note 13 (Application Note 12 from [4], refined by ST author)

The TOE (SimplySign SAM) configuration of cryptographic algorithm parameters is handled based on the list of accepted algorithms and their parameters.

R.Privileged_User: is a TOE subject containing the set of data that uniquely identifies a Privileged User within the TOE. It shall be protected in integrity.

R.Reference_Privileged_User_Authentication_Data: is the set of data used by the TOE to authenticate the Privileged User. It shall be protected in integrity and confidentiality.

Application Note 14 (Application Note 13 from [4], refined by ST author)

In the case of TOE (SimplySign SAM), R.Reference_Privileged_User_Authentication_Data is a TLS client certificate for SimplySign SSA.

R.Random: is random secrets, e.g. keys, used by the TOE to operate and communicate with external parties. It shall be protected in integrity and confidentiality.

3.2. Subjects

This following list of subjects interact with the TOE:

- Signer, which is the natural or legal person who uses the TOE through the SAP where they provide the SAD and can sign DTBS/R(s) using their signing key in the CM.
- Privileged User, which performs the administrative functions of the TOE and is able to supply DTBS/R(s) to the TOE as part of the signature operation.

Application Note 15 (from ST Author)

Signer is able to trigger a signing process: he authorises the signing key in the CM and provides the required data.

Application Note 16 (Application Note 14 from [4], refined by ST author)

The list of subjects described in EN 419 241-1 [2] clause 6.2.1.2 SRG M.1.2 contains more roles as it covers the whole T4WS.

The TOE (SimplySign SAM) implements two roles: Signer and Privileged User (SimplySign SSA), which are described in this ST.

Application Note 17 (Application Note 15 from [4], refined by ST author)

The SimplySign SSA is considered as Privileged User.

Application Note 18 (Application Note 16 from [4], refined by ST author)

The creation of signers, management of reference signer authentication data and signing key generation is configured to be carried out as specified in e.g. ETSI EN 319 411-1 [9].

3.3. Threats

3.3.1. General

The following threats are defined for the TOE. An attacker described in each of the threats is a subject that is not authorised for the relevant operation, but may present himself as an unknown user or as one of the other defined subjects.

3.3.2. Enrolment

The threats during enrolment are:

T.ENROLMENT_SIGNER_IMPERSONATION

An attacker impersonates Signer during enrolment. As examples, it could be:

- by transferring wrong R.Signer to TOE from RA,
- by transferring wrong R.Reference_Signer_Authentication_Data to TOE from RA.

The assets R.Signer and R.Reference_Signer_Authentication_Data are threatened.

Such impersonation may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

An attacker is able to obtain whole or part of R.Reference_Signer_Authentication_Data during enrolment. This can be during generation, storage or transfer to the TOE or transfer between the Signer and TOE. As examples, it could be:

- by reading the data
- by changing the data, e.g. to a known value

The asset R.Reference_Signer_Authentication_Data is threatened.

Such data disclosure may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

The threats on enrolment are threats on the environment in case external authentication is supported by the TOE.

T.SVD_FORGERY

An attacker modifies the R.SVD during transmission to the RA or CA. This results in loss of R.SVD integrity in the binding of R.SVD to the signing key and to R.Signer.

The asset R.SVD is threatened.

If the CA relies on the generation of the key pair controlled by the TOE as specified in ETSI EN 319 411-1 [9] clause 6.3.3 d) then an attacker can forge signatures masquerading as the Signer.

Application Note 19 (Application Note 17 from [4], refined by ST author)

The secure transport of R.SVD from TOE to RA or CA is provided by TLS.

3.3.3. Signer Management

T.ADMIN_IMPERSONATION

Attacker impersonates a Privileged User and updates R.Reference_Signer_Authentication_Data, R.Signing_Key_Id or R.SVD.

The assets R.Reference_Signer_Authentication_Data, R.SVD and R.Signing_Key_Id are threatened.

Such data modification may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

Attacker discloses or changes (e. g. to a known value) R.Reference_Signer_Authentication_Data during update and is able to create a signature.

The assets R.Reference_Signer_Authentication_Data and R.Signing_Key_Id are threatened.

Such data disclosure may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of Signer.

3.3.4. Usage

This section describes threats for signature operation including authentication.

T.AUTHENTICATION_SIGNER_IMPERSONATION

An attacker impersonates the Signer using forged R.Reference_Signer_Authentication_Data and transmits it to the TOE during SAP and uses it to sign the same or modified DTBS/R(s).

The assets R.Reference_Signer_Authentication_Data, R.SAD and R.Signing_Key_Id are threatened.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED

An attacker is able to modify R.Reference_Signer_Authentication_Data inside the TOE or during maintenance.

The asset R.Reference_Signer_Authentification_Data is threatened.

Such data modification may allow a potential incorrect Signer authentication leading to unauthorised signature operation on behalf of the Signer.

T.SAP_BYPASS

An attacker bypasses one or more steps in the SAP and is able to create a signature without the Signer having authorised the operation.

The asset R.SAD is threatened.

T.SAP_REPLAY

An attacker replays one or more steps of SAP and is able to create a signature without the Signer having authorised the operation.

The asset R.SAD is threatened.

T.SAD_FORGERY

An attacker forges or manipulates R.SAD during transfer in SAP and is able to create a signature without the Signer having authorised the operation.

The asset **R.SAD** is threatened.

T.SIGNATURE_REQUEST_DISCLOSURE

An attacker obtains knowledge of R.DTBS/R or R.SAD during transfer to TOE.

The asset R.DTBS/R and R.SAD is threatened.

If the R.DTBS/R or R.SAD do not require encrypted data then this threat is mitigated.

Application Note 20 (From ST Author)

This threat is mitigated, because R.DTBS/R is not encrypted - see Application Note 4.

T.DTBSR_FORGERY

An attacker modifies R.DTBS/R during transfer to TOE and is able to create a signature on this modified R.DTBS/R without the Signer having authorised the operation on this R.DTBS/R.

The asset R.DTBS/R is threatened.

T.SIGNATURE_FORGERY

An attacker modifies R.Signature during or after creation or during transfer outside the TOE.

The asset R.Signature is threatened.

Application Note 21 (Application Note 18 from [4])

The modification of a signature can be detected by the SSA or any relying party by validation of the signature.

3.3.5. System

T.PRIVILEGED_USER_INSERTION

An attacker is able to create R.Privileged_User including R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as a Privileged User.

The assets R.Privileged_User and R.Reference_Privileged_User_Authentication_Data are threatened.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION

An attacker modifies R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as the Privileged User.

The asset R.Reference_Privileged_User_Authentication_Data is threatened.

T.AUTHORISATION_DATA_UPDATE

Attacker impersonates Privileged User and updates R.Authorisation_Data or R.Authorisation_Data2 and may be able to activate a signing key.

The asset R.Authorisation_Data2, R.Authorisation_Data and R.Signing_Key_Id are threatened.

Application Note 22 (Application Note 19 from [4], refined by ST author)

Access to R.Authorisation_Data should only be allowed for authorized operators.

T. AUTHORISATION_DATA _DISCLOSE

Attacker discloses R.Authorisation_Data or R.Authorisation_Data2 during update and is able to activate a signing key.

The asset R.Authorisation_Data2, R.Authorisation_Data and R.Signing_Key_Id are threatened.

T.CONTEXT_ALTERATION

An attacker modifies system configuration R.TSF_DATA to perform an unauthorised operation.

The assets R.Signing_Key_Id, R.SVD, R.SAD, R.Reference_Signer_Authentication_Data and R.TSF_DATA are threatened.

T.AUDIT_ALTERATION

An attacker modifies system audit and is able hide trace of TOE modification or usage.

The assets R.SVD, R.SAD, R.Signer, R.Reference_Signer_Authentication_Data, R.DTBS/R, R.Signature, R.AUDIT and R.TSF_DATA are threatened.

T.RANDOM

An attacker is able to guess system secrets R.RANDOM and able to create or modify TOE objects or participate in communication with external systems.

3.4. Relation Between Threats & Assets

This following table provides an overview of the relationships between asset, associated security properties and threats. For details consult the individual threats in the previous sections.

Asset	Security Dimensions	Threats
R.Signing_Key_Id	Integrity	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Authorisation_Data	Integrity	T.AUTHORISATION_DATA_UPDATE
	Confidentiality	T.AUTHORISATION_DATA_UPDATE AUTHORISATION_DATA _DISCLOSE
R.Authorisation_Data2	Integrity	T.AUTHORISATION_DATA_UPDATE
	Confidentiality	T.AUTHORISATION_DATA_UPDATE AUTHORISATION_DATA _DISCLOSE
R.SVD	Integrity	T.SVD_FORGERY T.ADMIN_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
R.DTBS/R	Integrity	T.SIGNATURE_REQUEST_DISCLOSURE T.DTBSR_FORGERY
	Origin authentication	T.DTBSR_FORGERY
R.SAD	Integrity	T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION T.SAP_BYPASS T.SAP_REPLAY T.SAD_FORGERY
	Confidentiality	T.AUTHENTICATION_SIGNER_IMPERSONATION T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrity	T.SIGNATURE_FORGERY
R.Audit	Integrity	T.AUDIT_ALTERATION
R.Signer	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION
R.Reference_Signer_Authentication_Data	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Confidentiality	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Privileged_User	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.Reference_Privileged_User_Authentication_Data	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
	Confidentiality	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.RANDOM	Integrity	T.RANDOM
	Confidentiality	T.RANDOM
R.TSF_DATA	Integrity	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

Table 3-1 Relation between Assets, security properties & threats

3.5. Organisational Security Policies

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.RANDOM

The TOE is required to generate random numbers that meet a specified quality metric. These random numbers shall be suitable for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes.

OSP.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities as appropriate by TSPs. This includes generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

Application Note 23 (Application Note 20 from [4])

For cryptographic algorithms within the European Union this is as indicated in eIDAS [1] and an exemplary list of algorithms and parameters is given in ETSI TS 119 312 [11] or SOGIS [12].

3.6. Assumptions

A.PRIVILEGED_USER

It is assumed that all personnel administering the TOE are trusted, competent and possesses the resources and skills required for his tasks and is trained to conduct the activities he is responsible for.

A.SIGNER_ENROLMENT

The Signer shall be enrolled and certificates managed in conformance with the regulations given in eIDAS [1]. Guidance for how to implement an enrolment and certificate management system in conformance with eIDAS [1] are given in e.g. ETSI EN 319 411-1 [9] or for qualified certificate in e.g. ETSI EN 319 411-2 [14].

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

It is assumed that the Signer will not disclose his authentication factors.

A.SIGNER_DEVICE

It is assumed that the device and SIC used by Signer to interact with the SSA and the TOE is under the Signer's control for the signature operation, i.e. protected against malicious code.

A.CA

It is assumed that the qualified TSP that issues Signer qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in eIDAS [1].

A.ACCESS_PROTECTED

It is assumed that the TOE operates in a protected environment that limits physical access to the TOE to authorised Privileged Users. The TOE software and hardware environment (including client applications) is installed and maintained by Privileged Users in a secure state that mitigates against the specific risks applicable to the deployment environment.

It is assumed that any audit generated by the TOE are only handled by authorised personal in a physical secured environment. The personal that carries these activities should act under established practices.

It is assumed that where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities must provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment.

Application Note 24 (Application Note 21 from [4], refined by ST author)

Assets managed outside the TOE are protected in integrity and, when needed, confidentiality .

A.AUTH_DATA

It is assumed that the SAP is designed in such a way that the activation of the signing key is under sole control of the Signer with a high level of confidence. If SAD is received by the TOE, it shall be assumed that the SAD was submitted under the full control of the Signer by means that are in possession of the Signer.

A.TSP_AUDITED

It is assumed that the TSP deploying the SSA and TOE is a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [1] and audited to be compliant with the requirements for TSP's given by eIDAS [1] .

A.SEC_REQ

It is assumed that the TSP establishes an operating environment according to the security requirements for SCAL2 defined in EN 419 241-1 [2].

A.CERTIFICATION_AUTHORITY

It is assumed that the certificate for the R.SVD contains the R.SVD.

4. Security Objectives

4.1. General

This section identifies and defines the security objectives for the TOE and its operational environment. These security objectives reflect the stated intent, counter the identified threats, and take into account the assumptions.

4.2 Security objectives for the TOE

The following security objectives describe security functions to be provided by the TOE.

4.2.1. Enrolment

OT.SIGNER_PROTECTION

The TOE shall ensure that data associated to R.Signer is protected in integrity and if needed in confidentiality.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

The TOE shall be able to securely handle signer authentication data, R.Reference_Signer_Authentication_Data, as part of R.Signer.

OT.SIGNER_KEY_PAIR_GENERATION

The TOE shall be able to securely use the CM to generate Signer signing key pairs and assign R.Signing_Key_Id and R.SVD to R.Signer.

OT.SVD

The TOE shall ensure that the R.SVD linked to R.Signer is not modified before it is certified.

Application Note 25 (From ST author)

TOE verifies whether R.SVD is linked to R.Signer before Singer’s public key certificate is issued.

4.2.2. User Management

OT.PRIVILEGED_USER_MANAGEMENT

The TOE shall ensure that any modification to R.Privileged_User and R.Reference_Privileged_User_Authentication_Data are performed under control of a Privileged User.

OT.PRIVILEGED_USER_AUTHENTICATION

The TOE shall ensure that an administrator with a Privileged User is authenticated before any action on the TOE is performed.

Application Note 26 (Application Note 22 from [4])

The exception to this objective is when the initial (set of) Privileged Users are created as part of system initialisation.

OT.PRIVILEGED_USER_PROTECTION

The TOE shall ensure that data associated to R.Privileged_User are protected in integrity and if needed in confidentiality.

OT.SIGNER_MANAGEMENT

The TOE shall ensure that any modification to R.Signer, R.Reference_Signer_Authentication_Data, R.Signing_Key_Id and R.SVD are performed under control of the Signer or Privileged User.

4.2.3. Usage

OT.SAD_VERIFICATION

The TOE shall verify the SAD. That is, it shall check there is a link between the SAD elements and ensure the Signer is strongly authenticated.

Application Note 27 (Application Note 23 from [4], refined by ST author)

The TOE derives authorization data from authentication data in the SAD and uses this to activate the signing key in the CM.

Application Note 28 (Application Note 24 from [4])

Requirements for authentication are described in EN 419 241-1 [2], SRA_SAP.1.1.

OT.SAP

The TOE shall implement the server-side endpoint of a SAP, which provides the following:

- Signer authentication,
- Integrity of the transmitted SAD,
- Confidentiality of at least the elements of the SAD which contains sensitive information,
- Protection against replay, bypass of one or more steps and forgery.

Application Note 29 (Application Note 25 from [4], refined by ST author)

The signer authentication is assumed to be conducted according to EN 419241-1[2], SCAL.2 for qualified signatures.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION

The TOE shall ensure signature authentication data is protected against attacks.

OT.DTBSR_INTEGRITY

The TOE shall ensure that the R.DTBS/R is protected in integrity when transmitted to the TOE.

OT.SIGNATURE_INTEGRITY

The TOE shall ensure that a signature can't be modified inside the TOE.

OT.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities. This includes generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

4.2.4. System

OT.RANDOM

Random numbers generated used by the TOE for use as keys, in protocols or seed data for another random number generator that is used for these purposes shall meet a defined quality metric in order to ensure that random numbers are not predictable and have sufficient entropy.

OT.SYSTEM_PROTECTION

The TOE shall ensure that modification of R.TSF_DATA is authorised by Privileged User and that unauthorised modification can be detected.

OT.AUDIT_PROTECTION

The TOE shall ensure that modifications to R.AUDIT can be detected.

4.3. Security Objectives for the Operational Environment

OE.SVD_AUTHENTICITY

The operational environment shall ensure the SVD integrity during transmit outside the TOE to the CA.

OE.CA_REQUEST_CERTIFICATE

The operational environment shall ensure that the qualified TSP that issues qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in eIDAS [1].

The operational environment shall use a process for requesting a certificate, including SVD and Signer information, and CA signature in a way, which demonstrates the Signer is in control of the signing key associated with the SVD presented for certification. The integrity of the request shall be protected.

OE.CERTIFICATE_VERFICATION

The operational environment shall verify that the certificate for the R.SVD contains the R.SVD.

OE.SIGNER_AUTHENTICATION_DATA

The Signer's management of authentication factors data outside the TOE shall be carried out in a secure manner.

OE.DELEGATED_AUTHENTICATION

If the TOE has support for and is configured to use delegated authentication then the TSP deploying the SSA and TOE shall ensure that all requirements in EN 419 241-1 [2], SRA_SAP.1.1 are met.

In addition, the TSP shall ensure that:

- The delegated party fulfils all the relevant requirements of this standard and the requirements for registration according to the Regulation (EU) No 910/2014 [1], or
- The authentication process delegated to the external party uses an electronic identification means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of the Regulation (EU) No 910/2014 [1].

If the Signer is only authenticated using a delegated party, the TSP shall ensure that the secret key material used to authenticate the delegated party to the TOE shall reside in a certified CM consistent with the requirement as defined in EN 419 241-1 [2] SRG_KM.1.1.

The audit of the qualified TSP according to EN 419 241-1 [2] shall provide evidence that any delegated party meets requirements from EN 419 241-1[2] SRA_SAP.1.1. and optionally SRG_KM.1.1 in case the signer is only authenticated using a delegated party.

OE.DEVICE

The device, computer/tablet/smart phone containing the SIC and which is used by the Signer to interact with the TOE shall be protected against malicious code. It shall participate using SIC as local part of the SAP and may calculate SAD as described in EN 419 241-1 [2]. It may be used to view the document to be signed.

OE.ENV

The TSP deploying the SSA and TOE shall be a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [1] and audited to be compliant with the requirements for TSP's given by eIDAS [1]. The audit of the qualified TSP shall cover the security objectives for the operational environment specified in this clause.

The TOE shall operate in a protected environment that limits physical access to the TOE to authorised privileged users. The TOE software and hardware environment shall be installed and maintained by Privileged Users (System Administrators) in a secure state that mitigates against the specific risks applicable to the deployment environment, including (where applicable):

- Protection against loss or theft of the TOE or any of its externally stored assets.
- Inspections to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the TOE, or parts of the hardware appliance).
- Protection against the possibility of attacks based on emanations from the TOE, e.g. electromagnetic emanations, according to risks assessed for the operating environment.
- Protection against unauthorised software and configuration changes on the TOE and the hardware appliance.
- Protection to an equivalent level of all instances of the TOE holding the same assets, e.g. where a key is present as a backup in more than one instance of the TOE.

OE.CRYPTOMODULE_CERTIFIED

If the TOE is implemented as a local application within the same physical boundary as the cryptographic module defined in EN 419 221-5 [3] then the TOE relies on the cryptographic module for providing a tamper-protected environment and for cryptographic functionality and random number generation.

If the TOE is implemented within a separate physical boundary then the TOE relies on the cryptographic module for cryptographic functionality and random number generation. The physical boundary shall physically protect the TOE conformant to FPT_PHP.1 and FPT_PHP.3 in EN 419 221-5 [3].

Application Note 31 (Application Note 26 from [4], refined by ST author)

This ST does not claim conformance to EN 419 221-5 [3]. The TOE is implemented as a local application within the same physical appliance as the CM, and the crucial assets (private keys) are stored in the CM, which is certified and has its own tamper protection.

OE.TW4S_CONFORMANT

The TOE shall be operated by a qualified TSP in an operating environment conformant with EN 419241-1 [2].

4.4 Security Problem Definition & Security Objectives

The following tables map security objectives with the security problem definition.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	User Management	OT.PRIVILEGED_USER_MANAGEME NT	OT.PRIVILEGED_USER_AUTHENTICA TION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO
Enrolment																	
T.ENROLMENT_SIGNER_IMPERSONATION		X	X							X							
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		X	X														
T.SVD_FORGERY				X	X												X
Signer Management																	
T.ADMIN_IMPERSONATION								X		X							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE			X														
Usage																	
T.AUTHENTICATION_SIGNER_IMPERSONATION												X					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X										X	X			
T.SAP_BYPASS													X				
T.SAP_REPLAY													X				
T.SAD_FORGERY													X	X			
T.SIGNATURE_REQUEST_DISCLOSURE													X				
T.DTBSR_FORGERY															X		
T.SIGNATURE_FORGERY																X	X
System																	
T.PRIVILEGED_USER_INSERTION							X	X									
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							X	X	X								
T.AUTHORISATION_DATA_UPDATE																	
T.AUTHORISATION_DATA_DISCLOSE																	
T.CONTEXT_ALTERATION																	
T.AUDIT_ALTERATION																	
T.RANDOM																	
Organizational Security Policies																	
OSP.RANDOM																	
OSP.CRYPTO																	X

Table 4.1 TOE Security objectives (Enrolment, Signer Management, System) & (threats, Organizational Security Policies)

	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	Security Objectives for the Operational Environment	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT	OE.CERTIFICATE_VERFICATION	OE. DELEGATED_AUTHENTICATION
ENROLMENT														
T.ENROLMENT_SIGNER_ IMPERSONATION												X		X
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_ DISCLOSED								X	X					X
T.SVD_FORGERY						X	X							
SIGNER MANAGEMENT														
T.ADMIN_IMPERSONATION														
T.MAINTENANCE_AUTHENTICATION_DISCLOSE														X
USAGE														
T.AUTHENTICATION_SIGNER_ IMPERSONATION														
T.SIGNER_AUTHENTICATION_DATA_ MODIFIED														X
T.SAP_BYPASS									X					
T.SAP_REPLAY									X					
T.SAD_FORGERY								X	X					X
T.SIGNATURE_REQUEST_DISCLOSURE														
T.DTBSR_FORGERY									X					
T.SIGNATURE_FORGERY														
SYSTEM														
T.PRIVILEGED_USER_INSERTION														
T.REFERENCE_PRIVILEGED_USER_ AUTHENTICATION_DATA_ MODIFICATION														
T.AUTHORISATION_DATA_UPDATE			X											
T.AUTHORISATION_DATA_DISCLOSE			X											
T.CONTEXT_ALTERATION			X											
T.AUDIT_ALTERATION				X										
T.RANDOM		X												
ORGANIZATIONAL SECURITY POLICIES														
OSP.RANDOM		X												
OSP.CRYPTO											X			

Table 4.2 TOE Security objectives (Usage), Security Objectives for the Operational Environment & (threats, Organizational Security Policies)

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT	OE.CERTIFICATE_VERFICATION	OE. DELEGATED_AUTHENTICATION
Assumptions									
A.PRIVILEGED_USER							X		
A.SIGNER_ENROLMENT					X				
A.SIGNER_AUTHENTICATION_ DATA_PROTECTION			X						
A.SIGNER_DEVICE				X					
A.CA		X							
A.ACCESS_PROTECTED					X				
A.AUTH_DATA				X					
A.TSP_AUDITED					X				
A.SEC_REQ							X		
A.CERTIFICATION_AUTHORITY								X	

Table 4.3 TOE Assumptions and Security Objectives for the environment

4.5. Rationale for the Security Objectives

This section provides a rationale objective that covers each threat, organizational security policy and assumption.

4.5.4.1. Threats & Objectives

T.ENROLMENT_SIGNER_IMPERSONATION is covered by ***OT.SIGNER_PROTECTION*** requiring R.Signer to be protected in integrity and for sensitive parts in confidentiality.

It is also covered by ***OT.SIGNER_MANAGEMENT*** requiring the R.Signer to be securely created.

It is also covered by ***OT.REFERENCE_SIGNER_AUTHENTICATION_DATA*** requiring the TOE to be able to assign Signer authentication data to the R.Signer, as well as by ***OE.DELEGATED_AUTHENTICATION*** that requires the environment to protect Signer authentication data enrolment process, in the part relating to delegated authentication, in accordance with the standards applicable to the qualified TSP.

It is also covered by ***OE.TW4S_CONFORMANT*** as that requires signer enrolment to be handled in accordance with [18] for level at least substantial.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED is covered by ***OT.REFERENCE_SIGNER_AUTHENTICATION_DATA*** requiring that authentication data be securely handled, as well as by ***OE.DELEGATED_AUTHENTICATION*** that requires, in the part relating to delegated authentication, secure handling of authentication data, in accordance with the standards applicable to the qualified TSP.

It is also covered by ***OT.SIGNER_PROTECTION*** requiring that the attributes, including Signer authentication data, be protected in integrity and if needed in confidentiality.

It is also covered by ***OE.SIGNER_AUTHENTICATION_DATA*** requiring the Signer to keep his authentication data secret.

It is also covered by ***OE.DEVICE*** requiring the device used by the Signer not to disclose authentication data.

T.SVD_FORGERY is covered by ***OT.SIGNER_KEY_PAIR_GENERATION*** requiring a CM to generate Signer key pair.

It is also covered by ***OT.SVD*** requiring the SVD to be protected while inside the TOE.

It is also covered by ***OT.CRYPTO*** requiring the usage of endorsed algorithms.

It is also covered by ***OE.SVD_AUTHENTICITY*** requiring the environment to protect the SVD during transmit from the TOE to the CA.

It is also covered by ***OE.CA_REQUEST_CERTIFICATE*** requiring the certification request to be protected in integrity.

T.ADMIN_IMPERSONATION is covered by ***OT.SIGNER_MANAGEMENT*** and ***OT.PRIVILEGED_USER_AUTHENTICATION*** requiring any changes to the Signer representation and attributes are carried out in an authorised manner.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE is covered by ***OT.REFERENCE_SIGNER_AUTHENTICATION_DATA*** requiring that authentication data be securely handled, as well as by ***OE.DELEGATED_AUTHENTICATION*** that requires, in the part relating to delegated authentication, secure handling of authentication data, in accordance with the standards applicable to the qualified TSP.

T.AUTHENTICATION_SIGNER_IMPERSONATION is covered by ***OT.SAD_VERIFICATION*** requiring that the TOE checks the SAD received in the SAP.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED is covered by ***OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION*** requiring the SAD transported protected in the SAP.

It is also covered by ***OT.REFERENCE_SIGNER_AUTHENTICATION_DATA*** requiring that authentication data be securely handled, as well as by ***OE.DELEGATED_AUTHENTICATION*** that requires, in the part relating to delegated authentication, secure handling of authentication data, in accordance with the standards applicable to the qualified TSP.

It is also covered by ***OT.SAP*** requiring the integrity of the SAD is protected during transmit in the SAP.

T.SAP_BYPASS is covered by ***OT.SAP*** requiring that all steps, including SAD verification, of the SAP shall completed.

It is also covered by ***OE.DEVICE*** requiring the SIC to participate in the SAP.

T.SAP_REPLAY is covered by ***OT.SAP*** requiring that the SAP shall be able to resist whole or part of it being replayed.

It is also covered by ***OE.DEVICE*** requiring the SIC to participate in the SAP.

T.SIGNATURE_REQUEST_DISCLOSURE is covered by the ***OT.SAP*** requiring the protocol to be able to transmit data securely.

T.SAD_FORGERY is covered by ***OT.SAP*** requiring the TOE to be able to detect if the SAD has been modified during transmit to the TOE.

It is also covered by ***OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION*** requiring signature authentication data to be protected during transmit to the TOE, as well as by ***OE.DELEGATED_AUTHENTICATION*** that requires, in the part relating to delegated authentication, secure transmission of authentication data, in accordance with the standards applicable to the qualified TSP.

It is also covered by ***OE.SIGNER_AUTHENTICATION_DATA*** requiring the Signer to protect his authentication data.

It is also covered by ***OE.DEVICE*** requiring the device used by the Signer to participate correctly in the SAP, in particular the device shall not disclose authentication data.

T.DTBSR_FORGERY is covered by ***OT.DTBSR_INTEGRITY*** requiring the R.DTBS/R to be protected in integrity during transmit to the TOE.

It is also covered by ***OE.DEVICE*** requiring the SIC to participate in the SAP.

T.SIGNATURE_FORGERY is covered by ***OT.SIGNATURE_INTEGRITY*** requiring that the signature is protected in integrity inside the TOE.

It is also covered by ***OT.CRYPTO*** requiring the usage of endorsed algorithms.

T.PRIVILEGED_USER_INSERTION is covered by ***OT.PRIVILEGED_USER_MANAGEMENT*** requiring only Privileged User can create new R.Privileged_User and ***OT.PRIVILEGED_USER_AUTHENTICATION*** that requires a Privileged User to be authenticated.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION is covered by ***OT.PRIVILEGED_USER_MANAGEMENT*** requiring only Privileged User can modify R.Privileged_User and ***OT.PRIVILEGED_USER_AUTHENTICATION*** that requires a Privileged User to be authenticated.

It is also covered by ***OT.PRIVILEGED_USER_PROTECTION*** requiring the Privileged User to be protected in integrity.

T.AUTHORISATION_DATA_UPDATE is covered by ***OT.SYSTEM_PROTECTION*** requiring any unauthorised modification to TOE configuration to be detectable.

T.AUTHORISATION_DATA_DISCLOSE is covered by ***OT.SYSTEM_PROTECTION*** requiring any unauthorised modification to TOE configuration to be detectable.

T.CONTEXT_ALTERATION is covered by ***OT.SYSTEM_PROTECTION*** requiring any unauthorised modification to TOE configuration to be detectable.

T.AUDIT_ALTERATION is covered by ***OT.AUDIT_PROTECTION*** requiring any audit modification can be detected.

T.RANDOM is covered by ***OT.RANDOM*** requiring that random numbers are not predictable and have sufficient entropy.

4.5.4.2. Organizational Security Policies & Objectives

OSP.RANDOM is covered by ***OT.RANDOM*** requiring that random numbers are not predictable and have sufficient entropy.

OSP.CRYPTO is covered by ***OT.CRYPTO*** requiring the usage of endorsed algorithms and ***OE.CRYPTOMODULE_CERTIFIED*** requiring a CM to provide a tamper-protected environment and for cryptographic functionality and random number generation.

4.5.4.3. Assumptions & Objectives

A.PRIVILEGED_USER is covered by ***OE.TW4S_CONFORMANT*** which requires that the system where the TOE operates is compliant with EN 419 241-1 [2] where Clause SRG_M.1.8 requires that administrators are trained.

A.SIGNER_ENROLMENT is covered by ***OE.ENV*** requiring the TSP to be audited.

A.SIGNER_AUTHENTICATION_DATA_PROTECTION is covered by ***OE.SIGNER_AUTHENTICATION_DATA*** requiring the Signer to protect his authentication data.

A.SIGNER_DEVICE is covered by ***OE.DEVICE*** requiring the Signer's device to be protected against malicious code.

A.CA is covered by ***OE.CA_REQUEST_CERTIFICATE*** requiring that the CA will issue certificates containing the SVD.

A.ACCESS_PROTECTED is covered by ***OE.ENV*** requiring the TOE be operated in an environment with physical access controls.

A.AUTH_DATA is covered by ***OE.DEVICE*** requiring the device to participate correctly in the SAP.

A.TSP_AUDITED is covered by ***OE.ENV*** requiring that the TOE is operated by a qualified TSP.

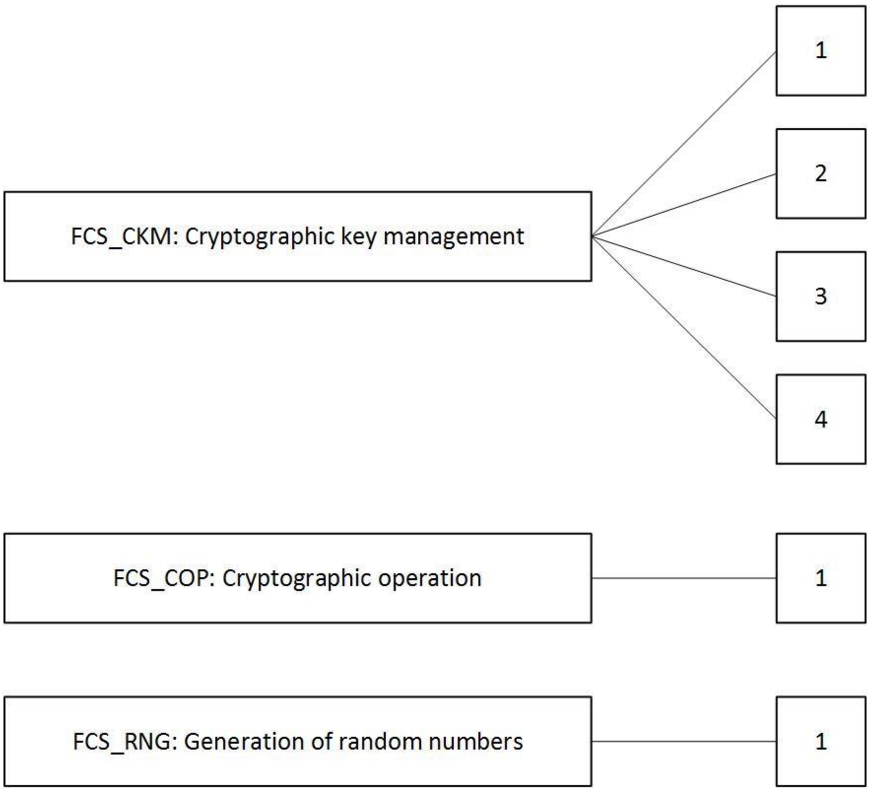
A.SEC_REQ is covered by ***OE.TW4S_CONFORMANT*** requiring the system where the TOE operates is compliant with EN 419 241-1 [2].

A.CERTIFICATION_AUTHORITY is covered by ***OE.CERTIFICATE_VERFICATION*** requiring the TOE be operated in an environment that verifies that the certificate for the R.SVD contains the R.SVD.

5. Extended Components Definition

5.1. Class FCS: Cryptographic Support

The Class FCS: Cryptographic Support as defined in [7] is extended with a new family: Generation of Random Numbers (FCS_RNG). The family is concerned with generation of random numbers. The following picture illustrates the decomposition of the Class FCS: Cryptographic Support with the added family FCS_RNG:


FCS_CKM: Cryptographic key management
1
2
3
4
FCS_COP: Cryptographic operation
1
FCS_RNG: Generation of random numbers
1

5.1.1. Generation of Random Numbers (FCS_RNG)

This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behaviour:

This family defines quality requirements for the generation of random numbers, which are intended to be used for cryptographic purposes.

Component levelling:

FCS_RNG: Generation of Random Numbers
1

Management: FCS_RNG.1

There are no foreseen management activities.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Generation of random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

Application Note 32 (Application Note 27 from [4])

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

6. Security Requirements

6.1. Typographical Conventions

The following conventions are used in the definitions of the SFRs:

- Refinements made in this ST are always updates of the text for the SFR. The added words are in **bold underlined text** and removed words are ~~crossed out~~.
- Selections made in this ST are written in **bold text and double underlined**, and the original text is indicated in a footnote.
- Assignments made in this ST are written in *italics and underlined*, and the original text is indicated in a footnote.
- Iterations made in this ST are denoted by a slash "/" and the **iteration indicator in bold text underlined** after the component identifier.

6.2. Subjects, Objects and Operations

This section describes the subjects, objects and operations supported by the TOE.

Subject	**Description**
R.Signer	Represents within the TOE, the end user that wants to create a digital signature
R.Privileged_User	Represents within the TOE a privileged user that can administer the TOE and a few operations relevant to R.Signer

Table 6.1. Subjects

Object	**Description**
R.Reference_Privileged_User_Authentication_Data	Data used by the TOE to authenticate a Privileged_User
R.Reference_Signer_Authentication_Data	Data used by the TOE to authenticate a Signer
R.SVD	The public part of a R.Signer signature key pair
R.Signing_Key_Id	An identifier representing the private part of a R.Signer signature key pair
R.DTBS/R	Data to be signed representation
R.Authorisation_Data	Data used by the CM to activate the private part of a R.Signer signature key pair
R.Authorisation_Data2	Data used by the TOE to change or reset PIN
R.Signature	The result of a signature operation

R.TSF_DATA	TOE Configuration Data

Table 6.2. Objects

Subject	Operation	Object	Description
R.Privileged_User	Create_New_ Privileged_User	R.Privileged_User R.Reference_Privileged_ User_Authentication_ Data	A new privileged user can be created which covers the object representing the new privileged user as well as the object used to authenticate the newly created privileged user.
R.Privileged_User	Create_New_Signer	R.Signer R.Reference_Signer_ Authentication_Data	A new signer can be created which covers the object representing the new signer as well as the object used to authenticate the newly created signer.
R.Privileged_User R.Signer	Generate_Signer_ Key_Pair	R.Signer R.SVD R.Signing_Key_Id	A key pair can be generated and assigned to a signer.
R.Privileged_User R.Signer	Signer_Maintenance	R.Signer R.SVD R.Signing_Key_Id	A key pair can be deleted from a signer.
R.Privileged_User	Supply_DTBS/R	R.Signer R.DTBS/R	Data to be signed by a signer can be supplied by a privileged user.
R.Signer	Signing	R.Authorisation_Data R.Signer R.Signing_Key_Id R.DTBS/R R.Signature	A signer can sign data to be signed resulting in a signature.
R.Privileged_User	TOE_Maintenance	R.TSF_DATA	The TOE configuration can be maintained by a privileged user

Table 6.3. Operations

Application Note 33 (From ST Autor)

The TOE allows only one Privileged User (SimplySing SSA), therefore an operation of creating a new Privileged User by an existing Privileged User is not applicable.

6.3. SFRs Overview

This section gives an overview of how the SFRs are related to handle TOE usage scenarios and Signer object.

Signer object

- FIA_ATD.1 and FIA_USB.1 requires that the R.Signer object is maintained by the TOE.
- FDP_ITC.2/Signer describes requirements for importing the R.Signer object.
- FDP_ETC.2/Signer describes requirements for exporting the R.Signer object.
- FDP_UIT.1 requires the R.Signer object to be protected in integrity when imported and exported.
- FPT_TDC.1 requires the TOE to be able to interpret R.Signer object related data when shared with the SSA.
- FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 describes rules for creation, maintaining and usage of the R.Signer object as well as requirements to its values.

Authentication

- FIA_AFL.1 limit the amount of authentication attempts
- FDP_UCT.1 ensure that access control and information flow data are transmitted in a confidential way.
- FIA_UID.2 and FIA_UAU.1 requires that each user is identified and authenticated before any action on behalf of the user can take place.
- FIA_UAU.5/Signer and FIA_UAU.5/Privileged User describe the list of authentication mechanism.

Create Signer

- FDP_ACC.1/Signer Creation using FDP_ACF.1/Signer Creation describes access control requirements for creating a R.Signer object.
- FIA_USB.1 defines authorisation rules for creating new R.Signer objects.

Signer Key Pair Generation

- FDP_ACC.1/Signer Key Pair Generation using FDP_ACF.1/Signer Key Pair Generation describes access control requirements for signing key pair generation.
- FCS_CKM.1/* describe rules for how signing key pair are generated.

Signer Key Pair Deletion

- FDP_ACC.1/Signer Key Pair Deletion using FDP_ACF.1/Signer Key Pair Deletion describes access control requirements for signing key pair deletion.
- FCS_CKM.4 requires keys to be securely destructed.

Signer Maintenance

- FDP_ACC.1/Signer Maintenance using FDP_ACF.1/Signer Maintenance describes access control requirements for updating the R.Reference_Signer_Authentication_Data of a R.Signer object.

Supply DTBS/R

- FDP_ACC.1/Supply DTBS/R using FDP_ACF.1/Supply DTBS/R describes access control requirements for a Privileged User to supply a DTBS/R(s).

Signing

- FDP_IFF.1/Signer and FDP_IFC.1/Signer describing requirements on preconditions for a signature operation can be carried out.
- FDP_UIT.1 requires the R.SAD object to be protected from modification and replay.
- FDP_ACC.1/Signing using FDP_ACF.1/Signing describes access control requirements for signing.
- FCS_COP.1/* requires the TOE to perform cryptographic operation conformant with a ST specified list of algorithms.
- FPT_RPL.1 requires detection of replay of the R.SAD and reject signature operation in case of replay detected.
- FPT_STM.1 is responsible for reliable time stamps for the signatures.

Privileged User object

- FIA_ATD.1 and FIA_USB.1 requires that the R.Privileged User object is maintained by the TOE**.**
- FDP_ITC.2/Privileged User describes requirements for importing the R.Privileged User object.
- FDP_ETC.2/Privileged User describes requirements for exporting the R.Privileged User object.
- FDP_UIT.1 requires the R.Privileged User object to be protected in integrity when imported and exported.
- FPT_TDC.1 requires the TOE to be able to interpret R.Privileged User object when shared with a trusted IT product the SSA.
- FMT_MSA.1, FMT_MSA.2 , FMT_MSA.3 describes rules for creation, maintaining and usage of the R.Privileged User object as well as requirements to its values.
- FDP_IFC.1/Privileged User and FDP_IFF.1/Privileged User describes rules accessing to the Privileged User's security attributes.

Privileged User Creation

- FDP_ACC.1/Privileged User Creation using FDP_ACF.1/Privileged User Creation describes access control requirements for creating a R.Privileged User object.
- FIA_USB.1 defines authorisation rules for creating new R.Privileged User objects.

TOE Maintenance

- FDP_ACC.1/TOE Maintenance using FDP_ACF.1/TOE Maintenance.
- FMT_SMF.1 and FMT_SMF.2 requires the TOE to be able to carry out management functions and maintain users and roles.

Audit

- FAU_GEN.1 and FAU_GEN.2 describes what shall be audited.

Communication

- FTP_TRP.1/SSA and FTP_TRP.1/SIC requires that either the Privileged User or the Signer initiates the communication.
- FTP_ITC.1/CM[1] requires trusted path for communication between TOE and the CM.

[1] Protection Profile [4] indicates here FTP_ITC.2, which is not later defined in the PP. ST authors correct it to FTP_ITC.1/CM

6.4. Security Functional Requirements

The individual security functional requirements are specified in the sections below.

6.4.1. Security Audit (FAU)

FAU_GEN.1 Audit 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 **not specified**[2] level of audit, and

c) Privileged User management;

d) Privileged User authentication;

e) Signer management;

f) Signer authentication;

g) Signing key generation;

h) Signing key destruction;

i) Signing key activation and usage including the hash of the DTBS/R(s) and R.Signature;

j) Change of TOE configuration;

k) None[3].

Application Note 34 (Application Note 28 from [4])

Management of R.Privileged User and R.Signer objects shall include all events, which creates, modifies or deletes the R.Signer or R.Privileged User objects.

Signer authentication shall include failed verification of an assertion provided by a delegated party.

TOE configuration shall include all events, which creates, modifies and deletes the configuration object.

Application Note 35 (Application Note 29 from [4])

Generation of a certification request is usage of the signing key and mandates an audit trail.

Application Note 36 (Application Note 30 from [4], refined by ST author)

The audit log for the signing operation contains the R.DTBS/R (s).

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the ST:

- ✓ *Type of action performed (success or failure),*
- ✓ *identity of the role which performs the operation,*
- ✓ *logID,*
- ✓ *operation status*[4]

[2] [selection: *minimum, basic, detailed, not specified*]

[3] [assignment: *other specifically defined auditable events*]

[4] [assignment: *Type of action performed (success or failure), identity of the role which performs the operation*. [assignment: *other audit relevant information*]]

Application Note 37 (Application Note 31 from [4])

Audit trail shall not include any data which allow to retrieve sensitive data like R.SAD, R.Reference_Signer_Authentication_Data, R.Authorisation_Data and and R.Authorisation_Data2.

In case of the TOE, audit trail does not include any data which allow to retrieve sensitive data.

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.

6.4.2. Cryptographic Support (FCS)

FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA*[5] and specified cryptographic key sizes *2048, 3072, 4096 bits* [6] that meet the following: *ETSI TS 119 312 [9], FIPS 186-4 [21], PKCS#1 [22]* [7].

FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.1.1/AES: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[8] and specified cryptographic key sizes *256 bits* [9] that meet the following: *ETSI TS 119 312 [9], SOG-IS [12]*[10].

Application Note 38 (Application Note 32 from [4])

The TOE is expected to use a CM certified in conformance with EN 419221-5:2016 [3], see also OE.CRYPTOMODULE_CERTIFIED for key generation. Although the TSF may not generate keys itself, this SFR expresses the requirement for the TSF to invoke the CM with the appropriate parameters whenever key generation is required.

Guidance on cryptographic algorithms can be found in ETSI TS 119 312 [11] and SOG-IS [12].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroize*[11] that meets the following: *FIPS 140-2 [15]*[12] .

Application Note 39 (Application Note 34 from [4], refined by ST author)

The TOE is expected to use a CM certified in conformance with EN 419221-5:2016 for key destruction.

FCS_COP.1/Signature Generation RSA - Cryptographic operation

FCS_COP.1.1/Signature Generation RSA: The TSF shall perform *generation of digital signature*[13] in accordance with a specified cryptographic algorithm *RSA*[14] and cryptographic key sizes *2048, 3072, 4096 bits*[15]

[5] [assignment: cryptographic key generation algorithm]
[6] [assignment: cryptographic key sizes]
[7] [assignment: list of standards]
[8] [assignment: cryptographic key generation algorithm]
[9] [assignment: cryptographic key sizes]
[10] [assignment: list of standards]
[11] [assignment: cryptographic key destruction method]
[12] [assignment: list of standards]
[13] [assignment: list of cryptographic operations]
[14] [assignment: cryptographic algorithm]
[15] [assignment: cryptographic key sizes]

that meet the following: *ETSI TS 119 312 [9], RSASSA-PKCS1-v1_5 and RSASSAPSS according to PKCS#1 [22] and FIPS 186-4 [21]*[16].

FCS_COP.1/Signature Verification RSA - Cryptographic operation

FCS_COP.1.1/Signature Verification RSA: The TSF shall perform *verification of digital signature*[17] in accordance with a specified cryptographic algorithm *RSA*[18] and cryptographic key sizes *2048, 3072, 4096 bits*[19] that meet the following: *ETSI TS 119 312 [9], RSASSA-PKCS1-v1_5 and RSASSAPSS according to PKCS#1 [22] and FIPS 186-4 [21]*[20].

FCS_COP.1/Message Digest - Cryptographic operation

FCS_COP.1.1/Message Digest: The TSF shall perform *message digest*[21] in accordance with a specified cryptographic algorithm *SHA1, SHA256, SHA384, SHA512*[22] and cryptographic key sizes *none*[23] that meet the following: *ETSI TS 119 312 [9] and FIPS 186-4 [21]*[24].

FCS_COP.1/Encryption Decryption - Cryptographic operation

FCS_COP.1.1/ Encryption Decryption: The TSF shall perform *encryption and decryption*[25] in accordance with a specified cryptographic algorithm *AES*[26] and cryptographic key sizes *256 bits*[27] that meet the following: *ETSI TS 119 312 [9], SOG-IS [12]*[28].

Application Note 40 (Application Note 36 from [4])

The TOE is expected to use a CM certified in conformance with EN 419221-5 [3] for cryptographic operations.

Application Note 41 (Application Note 37 from [4], refined by ST author)

The relevant authorities and endorsements for completion of the SFRs are determined by the context of the client applications that use the TOE. For digital signatures within the European Union, this is as indicated in Regulation (EU) No 910/2014 [1] and a list of approved signature and seal formats are given in [13].

FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1: The TSF shall provide a **hybrid deterministic**[29] random number generator that implements: *securing communication with CM*[30].

FCS_RNG.1.2: The TSF shall provide **octets of bits**[31] that meet *NIST 800-90A [16]*[32].

[16] [assignment: list of standards]
[17] [assignment: list of cryptographic operations]
[18] [assignment: cryptographic algorithm]
[19] [assignment: cryptographic key sizes]
[20] [assignment: list of standards]
[21] [assignment: list of cryptographic operations]
[22] [assignment: cryptographic algorithm]
[23] [assignment: cryptographic key sizes]
[24] [assignment: list of standards]
[25] [assignment: list of cryptographic operations]
[26] [assignment: cryptographic algorithm]
[27] [assignment: cryptographic key sizes]
[28] [assignment: list of standards]
[29] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[30] [assignment: list of security capabilities]
[31] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]
[32] [assignment: a defined quality metric]

Application Note 42 (Application Note 38 from [4])

For more information on the selections and assignments, see the SFR definition in section 5.1.1.

Application Note 43 (Application Note 39 from [4], refined by ST author)

TOE (SimplySign SAM) is implemented as an application within the same hardware appliance as the CM.

6.4.3. User Data Protection (FDP)

FDP_ACC.1/Privileged User Creation - Subset access control

FDP_ACC.1.1/Privileged User Creation : The TSF shall enforce the *Privileged User Creation SFP*[33] on:

Subjects: Privileged User

Objects: New security attributes for the Privileged User to be created.

Operations: Create_New_Privileged_User:

The TOE creates R.Privileged_User and R.Reference_Privileged_User_ Authentication_Data with information transmitted by Privileged User[34].

Application Note 44 (Application Note 40 from [4], refined by ST author)

TOE allows just only one Privileged User.

FDP_ACF.1/Privileged User Creation - Security attribute based access control

FDP_ACF.1.1/Privileged User Creation: The TSF shall enforce the *Privileged User Creation SFP*[35] to objects based on the following:

1) *whether the subject is a Privileged User authorized to create a new Privileged User*[36].

FDP_ACF.1.2/Privileged User Creation: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1) *Only a Privileged User who has been authorized for creation of new users can carry out the Create_New_Privileged_User operation*[37].

FDP_ACF.1.3/Privileged User Creation: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*[38].
FDP_ACF.1.4/Privileged User Creation: The TSF shall explicitly deny access of subjects to objects based on the following additional rule *None*[39].

Application Note 45 (From ST author)

TOE allows just only one Privileged User.

FDP_ACC.1/Signer Creation - Subset access control

[33] [assignment: access control SFP]
[34] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[35] [assignment: access control SFP]
[36] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[37] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[38] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[39] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_ACC.1.1/Signer Creation: The TSF shall enforce the *Signer Creation SFP*[40] on:

Subjects: Privileged User

Objects: R.Signer and R.Reference_Signer_Authentication_Data

Operations: Create_New_Signer:

The TOE creates R.Signer and R.Reference_Signer_Authentication_Data with information transmitted by Privileged User[41].

FDP_ACF.1/Signer Creation - Security attribute based access control

FDP_ACF.1.1/Signer Creation: The TSF shall enforce the *Signer Creation SFP*[42] to objects based on the following:

1) *whether the subject is a Privileged User authorized to create a new Signer*[43].

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

1) *Only a Privileged User who has been authorized for creation of new users can carry out the Create_New_Signer operation*[44].

FDP_ACF.1.3/Signer Creation: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*[45].

FDP_ACF.1.4/Signer Creation: The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None*[46].

FDP_ACC.1/Signer Maintenance - Subset access control

FDP_ACC.1.1/Signer Maintenance: The TSF shall enforce the *Signer Maintenance SFP*[47] on:

Subjects: Privileged User and Signer

Objects: The security attributes R.Reference_Signer_Authentication_Data of R.Signer

Operations: Signer_Maintenance:

The Privileged User or Signer instructs the TOE to update R.Reference_Signer_Authentication_Data of R.Signer [48].

FDP_ACF.1/Signer Maintenance - Security attribute based access control

FDP_ACF.1.1/Signer Maintenance: The TSF shall enforce the *Signer Maintenance SFP*[49] to objects based on the following:

[40] [assignment: access control SFP]

[41] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[42] [assignment: access control SFP]

[43] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[44] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[45] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[46] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[47] [assignment: access control SFP]

[48] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[49] [assignment: access control SFP]

1) *Whether the subject is a Privileged User or Signer authorized to maintain the Signer security attributes*[50].

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

1) *Only a Privileged User or Signer who has been authorized to maintain a Signer can carry out the Signer_Maintenance operation*[51].

FDP_ACF.1.3/Signer Maintenance: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1) *The Signer shall be the owner of the R.Signer object to be maintained*[52].

FDP_ACF.1.4/Signer Maintenance: The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1) *If the Signer does not own the R.Signer object, it can't be maintained*[53].

Application Note 46 (Application Note 41 from [4], refined by ST author)

In TOE, R.Reference_Signer_Authentication_Data cannot be maintained by a Signer.

FDP_ACC.1/Signer Key Pair Generation - Subset access control

FDP_ACC.1.1/Signer Key Pair Generation: The TSF shall enforce the *Signer Key Pair Generation SFP*[54] on:

Subjects: Privileged User and Signer.

Objects: The security attributes R.SVD and R.Signing_Key_Id as part of R.Signer.

Operations: Generate_Signer_Key_Pair:

The Privileged User or Signer instruct the TOE to request the Cryptographic Module to generate a signing key pair R.Signing_Key_Id and R.SVD and assign them to the R.Signer [55].

Application Note 47 (Application Note 42 from [4], refined by ST author)

R.Authorisation_Data is established by the CM when the key pair is generated on behalf of the Signer (see Application Note 2 in sec. 3.1 Assets).

Application Note 48 (Application Note 43 from [4], refined by ST author)

The Signer's signing keys are encrypted by the CM.

Application Note 49 (Application Note 44 from [4], refined by ST author)

The TOE does not use pre-generated keys.

Application Note 50 (Application Note 45 from [4])

The environment shall ensure, if needed, any transformation of R.SVD to a certification request and transport to CA.

[50] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[51] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[52] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[53] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[54] [assignment: access control SFP]
[55] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

FDP_ACF.1/Signer Key Pair Generation - Security attribute based access control

FDP_ACF.1.1/Signer Key Pair Generation: The TSF shall enforce the *Signer Key Pair Generation SFP*[56] to objects based on the following:

1) *whether the subject is a Privileged User or Signer authorized to generate a key pair*[57].

FDP_ACF.1.2/Signer Key Pair Generation: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1) *Only a Privileged User or Signer who has been authorized to generate the key pair can carry out the Generate_Signer_Key_Pair operation*[58].

FDP_ACF.1.3/Signer Key Pair Generation: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1) *The Signer must be the owner of the R.Signer object where the key pair is to be generated*[59].

FDP_ACF.1.4/Signer Key Pair Generation: The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1) *If the Signer does not own the R.Signer object, key pair shall not be generated*[60].

Application Note 51 (Application Note 46 from [4], refined by ST author)

The TOE does not use pre-generated keys.

Application Note 52 (Application Note 47 from [4])

Owning a R.Signer object is described in FIA_UAU.5/Signer.

FDP_ACC.1/Signer Key Pair Deletion - Subset access control

FDP_ACC.1.1/Signer Key Pair Deletion: The TSF shall enforce the *Signer Key Pair Deletion SFP*[61] on:

Subjects: Privileged User and Signer

Objects: The security attributes R.Signing_Key_Id and R.SVD of R.Signer

Operations: Signer_Key_Pair_Deletion:

The Privileged User or Signer instructs the TOE to delete the R.Signing_Key_Id and R.SVD of R.Signer[62].

Application Note 53 (Application Note 48 from [4], refined by ST author)

This SFR is limited to covering deletion of the R.Signing_Key_Id and R.SVD of R.Signer performed by the TOE and where authorisation to perform operations is managed by TOE.

FDP_ACF.1/Signer Key Pair Deletion Security attribute based access control

FDP_ACF.1.1/Signer Key Pair Deletion: The TSF shall enforce the *Signer Key Pair Deletion SFP*[63] to objects based on the following:

[56] [assignment: access control SFP]

[57] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[58] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[59] rules [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[60] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[61] [assignment: access control SFP]

[62] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[63] [assignment: access control SFP]

1) *Whether the subject is a Privileged User or Signer authorised to delete the Signer security attributes*[64].

FDP_ACF.1.2/Signer Key Pair Deletion: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1) *Only a Privileged User or Signer who has been authorised to delete a key pair can carry out the Signer_Key_Pair_Deletion operation*[65].

FDP_ACF.1.3/Signer Key Pair Deletion: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

1) *The Signer must be the owner of the R.Signer object containing the key pair to be deleted*[66].

FDP_ACF.1.4/Signer Key Pair Deletion: The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1) *If the Signer does not own the R.Signer object, the key pair can't be deleted*[67].

The DTBS/R(s) can be supplied to the TOE either by the Signer as part of the Signature Activation Protocol, which is covered by the FDP_ACC.1/Signing or by a Privileged User prior the signature operation. The following SFR handles the case where the Privileged User supplies the DTBS/R(s).

FDP_ACC.1/Supply DTBS/R - Subset access control

FDP_ACC.1.1/Supply DTBS/R: The TSF shall enforce the *Supply DTBS/R SFP*[68] on:

Subjects: Privileged User

Objects: The security attributes R.DTBS/R of R.Signer.

Operations: Supply_DTBS/R:

The Privileged User instructs the TOE to link the supplied DTBS/R(s) to the next signature operation for R.Signer[69].

Application Note 54 (Application Note 49 from [4], refined by ST author)

TOE does not provide facilities for Privileged User to supply the DTBS/R(s) then the relevant part of the SFR is trivially satisfied.

FDP_ACF.1/Supply DTBS/R - Security attribute based access control

FDP_ACF.1.1/Supply DTBS/R: The TSF shall enforce the *Supply DTBS/R SFP*[70] to objects based on the following:

1) *Whether the subject is a Privileged User authorized to supply a DTBS/R(s)*[71].

FDP_ACF.1.2/Supply DTBS/R: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[64] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[65] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[66] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[67] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[68] [assignment: access control SFP]

[69] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[70] [assignment: access control SFP]

[71] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

1) *Only a Privileged User who has been authorized to supply a DTBS/R(s) can carry out the Supply_DTBS/R operation*[72].

FDP_ACF.1.3/Supply DTBS/R: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*[73].

FDP_ACF.1.4/Supply DTBS/R: The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None*[74].

Application Note 55 (Application Note 50 from [4], refined by ST author)

TOE does not provide facilities for Privileged User to supply the DTBS/R(s) then the relevant part of the SFR is trivially satisfied.

FDP_ACC.1/Signing - Subset access control

FDP_ACC.1.1/ Signing: The TSF shall enforce the *Signing SFP*[75] on:

Subjects: Signer

Objects: R.Authorisation Data, security attributes, R.Signing_Key_Id and R.DTBS/R of R.Signer and R.Signature.

Operations: Signing:

The Signer instructs the TOE to perform a signature operation containing the following steps:

- *The TOE establishes R.Authorisation_Data for the R.Signing_Key_Id.*
- *The TOE uses the R.Authorisation_Data and R.Signing_Key_Id to activate a signing key in the Cryptographic Module and signs the R.DTBS/R(s) resulting in R.Signature,*
- *The TOE deactivates the signing key when the signature operation is completed*[76].

Application Note 56 (Application Note 51 from [4], refined by ST author)

CM actives signing keys after successful verification of R.Authorisation_Data (PIN).

Application Note 57 (Application Note 52 from [4], refined by ST author)

The Signing Application (SCA) provides the DTBS/R(s) to SimplySign SSA which passes it to the TOE via SAP as a component of signing process. R.DTBS/R(s) is contained into the R.SAD.

Application Note 58 (Application Note 53 from [4])

Signing key deactivating means that the Signer shall authorize any subsequent use of it.

FDP_ACF.1/Signing - Security attribute based access control

FDP_ACF.1.1/Signing: The TSF shall enforce the *Signing SFP*[77] to objects based on the following:

1) *Whether the subject is a Signer authorized to create a signature*[78].

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

[72] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[73] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[74] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[75] [assignment: access control SFP]
[76] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[77] [assignment: access control SFP]
[78] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

1) *The R.SAD is verified in integrity.*

2) *The R.SAD is verified that it binds together the Signer authentication, a set of R.DTBS/R and R.Signing_Key_Id.*

3) *The R.DTBS/R(s) used for signature operations is bound to the R.SAD.*

4) *The Signer identified in the SAD is authenticated according to the rules specified in FIA_UAU.5/Signer.*

5) Only an R.Signing_Key_Id as bound in the SAD, and which is part of the R.Signer security attributes, can be used to create a signature[79].

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

1) The Signer must be the owner of the R.Signer object used to generate the signature[80].

FDP_ACF.1.4/Signing: The TSF shall explicitly deny access of subjects to objects based on the following additional rule:

1) *If the Signer does not own the R.Signer object, it can't be used to create a signature*[81].

Application Note 59 (Application Note 54 from [4], refined by ST author)

The TOE does not work with default keys, therefore the R.Signing_Key_Id is not implied but indicated by R.SAD.

FDP_ACC.1/TOE Maintenance - Subset access control

FDP_ACC.1.1/TOE Maintenance: The TSF shall enforce the *TOE Maintenance SFP*[82] on:

Subjects: Privileged User

Objects: R.TSF_DATA.

Operations: TOE_Maintenance:

The Privileged User transmits information to the TOE to manage R.TSF_DATA[83].

FDP_ACF.1/TOE Maintenance - Security attribute based access control

FDP_ACF.1.1/TOE Maintenance: The TSF shall enforce the *TOE Maintenance SFP*[84] to objects based on the following:

1) Whether the subject is a Privileged User authorized to maintain the TOE configuration data[85].

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

1) Only a Privileged User who has been authorized to maintain the TOE can carry out the TOE_Maintenance operation[86].

[79] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[80] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[81] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[82] [assignment: access control SFP]

[83] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[84] [assignment: access control SFP]

[85] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[86] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

FDP_ACF.1.3/TOE Maintenance: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*[87].

FDP_ACF.1.4/TOE Maintenance: The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None*[88].

The TOE can store data in an external repository to meet requirements on, e.g. capacity and redundancy.

FDP_ETC.2/Signer - Export of user data with security attributes

FDP_ETC.2.1/Signer: The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion SFP, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP*[89] when exporting user data, controlled under the SFP(s), outside of the TSF.

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

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

FDP_ETC.2.4/Signer: The TSF shall enforce the following rules when user data are exported from the TOE*: None*[90].

Application Note 61 (Application Note 55 from [4], refined by ST author)

The TOE exports user data: Signer public key (R.SVD), and the result of the signature operation (R.Signature).

FDP_IFC.1/Signer - Subset information flow control

FDP_IFC.1.1/Signer: The TSF shall enforce the *Signer Flow SFP*[91] on *Privileged User and Signer accessing Signer security attributes for all operations*[92].

FDP_IFF.1/Signer - Simple security attributes

FDP_IFF.1.1/Signer: The TSF shall enforce the *Signer Flow SFP*[93] based on the following types of subject and information security attributes:

> *Privileged User and Signer accessing the Signer security attributes*[94].

FDP_IFF.1.2/Signer: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold*:*

> *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance.*
>
> *To allow a Signer to sign, the Signer shall be created in the TOE by FDP_ACC.1/Signer Creation followed by FDP_ACC.1/Signer key Pair Generation.*
>
> *After Signer is created the following operations can be done: FDP_ACC.1/Signer Key Pair Generation, FDP_ACC.1/Signer Key Pair Generation, FDP_ACC.1/Signer Maintenance and FDP_ACC.1/Signing*[95].

FDP_IFF.1.3/Signer: The TSF shall enforce the*: None*[96].

[87] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[88] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[89] [assignment: access control SFP(s) and/or information flow control SFP(s)]

[90] [assignment: additional exportation control rules]

[91] [assignment: information flow control SFP]

[92] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

[93] [assignment: information flow control SFP]

[94] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

[95] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

[96] [assignment: additional information flow control SFP rules]

FDP_IFF.1.4/Signer: The TSF shall explicitly authorize an information flow based on the following rules*: None*[97].
FDP_IFF.1.5/Signer: The TSF shall explicitly deny an information flow based on the following rules*: None*[98].

FDP_ETC.2/Privileged User - Export of user data with security attributes

FDP_ETC.2.1/Privileged User: The TSF shall enforce the *Privileged User Creation SFP*[99] when exporting user data, controlled under the SFP(s), outside of the TSF.

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

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

FDP_ETC.2.4/Privileged User: The TSF shall enforce the following rules when user data are exported from the TOE*: None*[100].

Application Note 62 (Application Note 56 from [4], refined by ST author)

The TOE does not export any Privileged User data, so the relevant part of the SFR is trivially satisfied.

FDP_IFC.1/Privileged User - Subset information flow control

FDP_IFC.1/Privileged User: The TSF shall enforce the *Privileged User Flow SFP*[101] on:

> *Privileged User accessing Privileged User security attributes for all operations*[102].

FDP_IFF.1/Privileged User - Simple security attributes

FDP_IFF.1.1/Privileged User: The TSF shall enforce the *Privileged User Flow SFP*[103] based on the following types of subject and information security attributes:

> *Privileged User accessing the Privileged User security attributes*[104].

FDP_IFF.1.2/Privileged User: The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold*:*

> *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance*[105].

FDP_IFF.1.3/Privileged User: The TSF shall enforce the*: None*[106].

FDP_IFF.1.4/Privileged User: The TSF shall explicitly authorize an information flow based on the following rules: *None*[107].

[97] [assignment: rules, based on security attributes, that explicitly authorise information flows]
[98] [assignment: rules, based on security attributes, that explicitly deny information flows]
[99] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[100] [assignment: additional exportation control rules]
[101] [assignment: information flow control SFP]
[102] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]
[103] [assignment: information flow control SFP]
[104] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]
[105] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[106] [assignment: additional information flow control SFP rules]
[107] [assignment: rules, based on security attributes, that explicitly authorise information flows]

FDP_IFF.1.5/Privileged User: The TSF shall explicitly deny an information flow based on the following rules: *None*[108].

FDP_ITC.2/Signer - Import of user data with security attributes

FDP_ITC.2.1/Signer: The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion SFP, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP*[109] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/Signer: The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Signer: The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Signer: The TSF shall ensure that interpretation of the security attributes of the imported user data are as intended by the source of the user data.

FDP_ITC.2.5/Signer: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *None*[110].

Application Note 63 (Application Note 57 from [4], refined by ST author)

In order to associate the Signer with the R.Signer, R.Authorization_Data (PIN) and R.Authorization_Data2 are imported to TOE from SimplySign SSA.

FDP_ ITC.2/Privileged User - Import of user data with security attributes

FDP_ITC.2.1/Privileged User: The TSF shall enforce the *Privileged User Creation SFP*[111] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/Privileged User: The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/Privileged User: The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/Privileged User: The TSF shall ensure that interpretation of the security attributes of the imported user data are as intended by the source of the user data.

FDP_ITC.2.5/Privileged User: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *None*[112].

Application Note 64 (Application Note 58 from [4], refined by ST author)

The TOE does not import any Privileged User data, so the relevant part of the SFR is trivially satisfied.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1: The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP*[113] to *transmit and receive*[114] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

[108] [assignment: rules, based on security attributes, that explicitly deny information flows]
[109] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[110] [assignment: additional importation control rules]
[111] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[112] [assignment: additional importation control rules]
[113] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[114] [selection: transmit, receive]

FDP_UIT.1.1: The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP*[115] to *transmit and receive*[116] user data in a manner protected from *modification and insertion*[117] errors **for R.Signer and R.Privileged User and for R.SAD also**[118] from *modification and replay*[119] errors.

FDP_UIT.1.2: The TSF shall be able to determine on receipt of user data, whether *modification, deletion and insertion*[120] **for R.Signer and R.Privileged_User and for R.SAD**[121] *whether modification and replay*[122] has occurred.

Application Note 65 (Application Note 59 from [4])

Insertion of objects would mean that authorised creation of Signer and Privileged User could be possible.

6.4.4. Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1: The TSF shall detect when **3**[123] unsuccessful authentication attempts occur related to ~~Privileged User and~~ Signer authentication[124].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been *met*[125], the TSF shall *~~suspend the Privileged User and when it is a Signer~~ suspend the usage of R.Signing_Key_Id*[126].

Application Note 66 (Application Note 60 from [4], refined by ST author)

Unsuccessful authentication attempts with PIN blocks the usage of R.Signing_Key_Id.

Application Note 67 (Application Note 61 from [4], refined by ST author)

The SFR only applies when the TOE uses any direct authentication.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users: *the security attribute as defined in FIA_USB.1*[127].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1: The TSF shall allow: *None*[128] on behalf of the user to be performed before the user is authenticated.

[115] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[116] [selection: transmit, receive]
[117] [selection: modification, deletion, insertion, replay]
[118] The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.
[119] [selection: modification, deletion, insertion, replay]
[120] [selection: modification, deletion, insertion, replay]
[121] The TSF shall be able to determine on receipt of user data, whether [selection: modification, deletion, insertion, replay] has occurred
[122] [selection: modification, deletion, insertion, replay]
[123] [selection: [assignment: positive integer number], a TOE Maintenance configurable positive integer within [assignment: range of acceptable values]]
[124] [assignment: list of authentication]
[125] [selection: met, surpassed]
[126] [assignment: list of actions]
[127] [assignment: list of security attributes]
[128] [assignment: list of TSF mediated actions**]**

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

FIA_UAU.5/Signer - Multiple authentication mechanisms

FIA_UAU.5.1/Signer: The TSF shall provide R.Authorization.Data validation, R.Authorization.Data2 validation, assertion validation[129] **to support Signer authentication**[130].

FIA_UAU.5.2/Signer: The TSF shall authenticate any **Signer's**[131] claimed identity according to:

- **SVD of SimplySign SSA is used to verify an assertion provided as a result of delegated authentication (Factor 1), and**
- **the Signer provides PIN (Factor 2) to activate signing Key in the CM,**
- **the Signer provides R.Authorisation_Data 2 to change/reset Signer's PIN**[132]**.**

Application Note 68 (Application Note 62 from [4], refined by ST author)

Successful authentication gives Signer access to the relevant R.Signer object as the owner.

The R.Authorisation_Data2 –is only used to change/reset PIN.

FIA_UAU.5/Privileged User - Multiple authentication mechanisms

FIA_UAU.5.1/Privileged User: The TSF shall provide *TLS client certificate authentication*[133] to support **Privileged User**[134] authentication.

FIA_UAU.5.2/Privileged User: The TSF shall authenticate any **Privileged** user's claimed identity according to the: *Privileged User TLS authentication certificate*[135].

Application Note 69 (from ST author)

Privileged User is authenticated by TLS client certificate.

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_USB.1 User-subject binding

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

1) *R.Reference_Signer_Authentication_Data*

[129] [selection: [assignment: list of direct authentication mechanisms conformant to EN 419 241-1 [2] SRA_SAP.1.1], [assignment: list of delegated authentication mechanisms conformant to EN 419 241-1 [2] SRA_SAP.1.1]]

[130] The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.

[131] user

[133] [assignment: list of authentication mechanisms]

[134] user

[135] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

2) *R.Signing_Key_Id*

3) *R.SVD*

4) *R.Signer*

5) *R.Auhorization_Data*

6) *R.Auhorization_Data2*[136]

to Signer

1) *R.Reference_Priviliged_User_Authentication_Data*

2) *R.Privileged_User*[137]

to Privileged User.

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1) *Whether the subject is a Privileged User (SimplySign SSA) authorized to create a new Signer.*

2) *Whether the subject is a Privileged User authorized to create a new Privileged User*.

3) *None*[138].

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

1) *Whether the subject is a Privileged User authorized to modify an R.Signer object.*

2) *Whether the subject is a Signer authorized to modify his own R.Signer object.*

3) *None*[139].

Application Note 70 (Application Note 63 from [4])

In FIA_USB.1.2 several attributes including R.Signing_Key_ID, R.SVD and R.DTBS/R may initially be empty.

Application Note 71 (Application Note 64 from [4], refined by ST author)

R.Authorisation_Data and R.Authorization_Data2 are included in FIA_USB.1.1. The assets are detailed in Application Notes in sec. 3.1.

Application Note 72 (Application Note 65 from [4], refined by ST author)

Signer Application (SCA) provides the R.DTBS/R to SimplySign SSA which passes it to the TOE for signature computation. R.DTBS/R is not considered as a Signer attribute.

6.4.5. Security Management (FMT)

FMT_MSA.1/Signer - Management of security attributes

FMT_MSA.1.1/Signer: The TSF shall enforce the:

1) *Signer Creation SFP*[140] to restrict the ability to *create*[141] the security attributes *listed in FIA_USB.1 for Signer*[142] to *authorized Privileged User*[143].

[136] [assignment: list of user security attributes]
[137] [assignment: list of user security attributes]
[138] [assignment: rules for the initial association of attributes, [assignment: rules for the initial association of attributes]]
[139] [assignment: rules for the changing of attributes, [assignment: rules for the changing of attributes]]
[140] [assignment: access control SFP(s), information flow control SFP(s)]
[141] [selection: change, default, query, modify, delete [assignment: other operations]]
[142] [assignment: list of security attributes]
[143] [assignment: the authorised identified roles]

2) *Generate Signer Key Pair SFP*[144] to restrict the ability to *generate*[145] the security attributes *R.SVD and R.Signing_Key_Id*[146] to *authorized Privileged User and Signer*[147].

3) *Signer Key Pair Deletion SFP*[148] to restrict the ability to *destruct*[149] the security attributes *R.SVD and R.Signing_Key_Id as part of R.Signer*[150] to *authorized Signer*[151].

4) *Supply DTBS/R SFP*[152] to restrict the ability to *create*[153] the security attribute *R.DTBS/R as part of R.Signer*[154] to *authorized Privileged User*[155]

5) *Signing SFP*[156] to restrict the ability to *create*[157] the security attributes *R.DTBS/R as part of R.Signer*[158] to *authorized Signer*[159].

6) *Signing SFP*[160] to restrict the ability to *query*[161] the security attributes *as listed in FIA_USB.1*[162] to *authorized Signer*[163].

7) *Signer Maintenance SFP*[164] to restrict the ability to *change*[165] the security attributes *R.Reference_Signer_Authentication Data*[166] *as part of R.Signer* to *authorized Privileged User and Signer*[167].

Application Note 73 (From ST author)

TOE does not provide facilities for Privileged User to supply the DTBS/R(s).

FMT_MSA.1/Privileged User - Management of security attributes

FMT_MSA.1.1/ Privileged User: The TSF shall enforce the

(1) *Privileged User Creation SFP*[168] to restrict the ability to *create and query*[169] the security attributes *listed in FIA_USB.1 for Privileged User*[170] to *authorized Privileged User*[171].

Application Note 74 (from ST author)

Privileged User is created only when the TOE is initialized.

[144] [assignment: access control SFP(s), information flow control SFP(s)]
[145] [selection: change, default, query, modify, delete [assignment: other operations]]
[146] [assignment: list of security attributes]
[147] [assignment: the authorised identified roles]
[148] [assignment: access control SFP(s), information flow control SFP(s)]
[149] [selection: change, default, query, modify, delete [assignment: other operations]]
[150] [assignment: list of security attributes]
[151] [assignment: the authorised identified roles]
[152] [assignment: *access control SFP(s), information flow control SFP(s)*]
[153] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[154] [assignment: list of security attributes]
[155] [assignment: *list of security attributes*]
[156] [assignment: access control SFP(s), information flow control SFP(s)]
[157] [selection: change, default, query, modify, delete [assignment: other operations]]
[158] [assignment: list of security attributes]
[159] [assignment: the authorised identified roles]
[160] [assignment: access control SFP(s), information flow control SFP(s)]
[161] [selection: change, default, query, modify, delete [assignment: other operations]**]**
[162] [assignment: list of security attributes]
[163] [assignment: the authorised identified roles]
[164] [assignment: access control SFP(s), information flow control SFP(s)]
[165] [selection: change, default, query, modify, delete: [assignment: other operations:**]**
[166] [assignment: list of security attributes]
[167] assignment: the authorised identified roles]
[168] [assignment: access control SFP(s), information flow control SFP(s)]
[169] [selection: change, default, query, modify, delete [assignment: other operations]**]**
[170] [assignment: *list of security attributes***]**
[171] [assignment: the authorised identified roles:]

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1: The TSF shall ensure that only secure values are accepted for *all security attributes listed in FIA_USB.1*[172].

FMT_MSA.3/Signer - Static attribute initialisation

FMT_MSA.3.1/ Signer: The TSF shall enforce the *Signer Creation SFP*[173] to provide *restrictive*[174] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ Signer: The TSF shall allow the *Privileged User*[175] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Privileged User - Static attribute initialisation

FMT_MSA.3.1/ Privileged User: The TSF shall enforce the *Privileged User Creation SFP*[176] to provide *restrictive*[177] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ Privileged User: The TSF shall allow the *Privileged User*[178] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1: The TSF shall restrict the ability to *modify*[179] the *R.TSF_DATA*[180] to *Privileged User*[181].

Application Note 75 (Application Note 66 from [4])

The TSF data includes configuration of System Administrator roles.

FMT_SMF.1 Specification of Management Functions

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

1) *Signer management,*
2) *Privileged User management*
3) *Configuration management*
4) *None*[182].

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1: The TSF shall maintain the roles *Signer and Privileged User*[183]**,** none[184].

[172] [assignment: list of security attributes]
[173] [assignment: access control SFP, information flow control SFP]
[174] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[175] [assignment: the authorised identified roles]
[176] [assignment: access control SFP, information flow control SFP]
[177] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[178] [assignment: the authorised identified roles]
[179] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[180] [assignment: list of TSF data]
[181] assignment: the authorised identified roles]
[182] [assignment: additional list of management functions to be provided by the TSF]
[183] [assignment: authorized identified roles]
[184] [assignment: other authorized identified roles]

FMT_SMR.2.2: The TSF shall be able to associate users with roles.

FMT_SMR.2.3: The TSF shall ensure that the conditions *Signer can't be a Privileged User*[185] are satisfied.

Application Note 76 (Application Note 67 from [4], refined by ST author)

Two roles are defined in the TOE: a Privileged User and a Signer. The description can be found in section 3.2.

6.4.6. Protection of the TSF (FPT)

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1: The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2: The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note 77 (Application Note 68 from [4], refined by ST author)

Because of the requirement for a physically secure environment with regular inspections (cf. OE.ENV), the level of protection (and hence resistance to attack potential) that is required by the implementation of FPT_PHP.1 for this TOE is equivalent to the physical security mechanisms for tamper detection and response required by section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements for each physical security embodiment in ISO/IEC 19790 [17] for Security Level 3. The level of physical protection that meet FPT_PHP.1 is also defined by reference to EN 419 241-1 [2] (cf. OE.TW4S_CONFORMANT), which subsequently refers to ETSI EN 319 401 [10] (section 7.6) regarding physical and environmental security requirements for the system operated by qualified TSP.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1: The TSF shall resist *physical manipulation*[186] to the *hard opaque potted enclosure of the CM*[187] by responding automatically such that the SFRs are always enforced.

Application Note 78 (Application Note 69 from [4], refined by ST author)

The TOE is implemented as a local application within the same physical appliance as the CM defined in EN 419-221-5 [3]. The crucial assets are managed by the CM, and so the SFRs FTP_PHP.* relies on the similar SFRs described for the CM, which is certified and has its own tamper protection.

Application Note 79 (Application Note 70 from [4], refined by ST author)

This SFR is linked to the requirements for passive detection of physical attacks in FPT_PHP.1, and should identify the relevant responses of the TOE involved in meeting the key zeroization requirements of [ISO/IEC 19790] Security Level 3. As in the case of FPT_PHP.1, because of the requirement for a physically secure environment with regular inspections (cf. OE.ENV), the level of protection (and hence resistance to attack potential) that is required by the implementation of FPT_PHP.3 for this TOE is equivalent to the level of assessment for this aspect of tamper detection and response required for section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements by each physical security embodiment in [ISO/IEC 19790 [17]] for Security Level 3. The level of physical protection that meet FPT_PHP.1 is also defined by reference to EN 419 241-1 [2] (cf. OE.TW4S_CONFORMANT), which subsequently refers to ETSI EN 319 401 [10] (section 7.6) regarding physical and environmental security requirements for the system operated by qualified TSP.

FPT_RPL.1 Replay detection

FPT_RPL.1.1: The TSF shall detect replay for the following entities *R.SAD*[188].

[185] [assignment: conditions for the different roles]

[186] [assignment: physical tampering scenarios]

[187] [assignment: list of TSF devices/elements]

[188] [assignment: list of identified entities]

FPT_RPL.1.2: The TSF shall perform *reject the signature operation*[189] when replay is detected.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps.

Application Note 80 (Application Note 71 from [4], refined by ST author)

The environment is integrated with the NTP server (has connection to 2 external time sources: tempus1.gum.gov.pl and tempus2.gum.gov.pl.). The time synchronisation is based on the NTP protocol.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1: The TSF shall provide the capability to consistently interpret:

1) *R.Signer,*
2) *R.Reference_Signer_Authentication_Data,*
3) *R.SAD,*
4) *R.DTBS/R,*
5) *R.SVD,*
6) *R.Privileged_User*
7) *R.Reference_Privileged_User_Authentication_Data*
8) *R.TSF_DATA*[190].

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2: The TSF shall use *data integrity either on data or on communication channel*[191] when interpreting the TSF data from another trusted IT product.

Application Note 81 (Application Note 72 from [4])
The SFR is used to handle the situation where the whole or part of the above data are stored outside the TOE.

6.4.7. Trusted Paths/Channels (FTP)

FTP_TRP.1/SSA - Inter-TSF Trusted path

FTP_TRP.1.1/SSA: The TSF shall provide a communication path between itself and ***Privileged User through SSA***[192] users that is logically distinct from other communication paths and provides ensured identification of its end points and protection of the communicated data from *modification*[193].

FTP_TRP.1.2/SSA: The TSF shall permit ***Privileged User through SSA***[194] to initiate communication via the trusted path.

FTP_TRP.1.3/SSA: The TSF shall require the use of the trusted path for*:*

1) *FDP_ACC.1.1/Privileged User Creation,*
2) *FDP_ACC.1/Signer Creation*
3) *FDP_ACC.1/Signer Maintenance*

[189] [assignment: list of specific actions]
[190] [assignment: list of TSF data types]
[191] [assignment: list of TSF data types]
[192] [selection: remote, local]
[193] [selection: modification**]**
[194] [selection: the TSF, local users, remote users]

4) *FDP_ACC.1/Signer Key Pair Generation*

5) *FDP_ACC.1/Signer Key Pair Deletion*

6) *FDP_ACC.1/Supply DTBS/R*

7) *FDP_ACC.1/TOE Maintenance*

8) *None*[195].

Application Note 82 (Application Note 73 from [4], refined by ST author)

Since it is not all data transmitted to the TOE that needs to be protected in confidentiality, FTP_TRP.1/ SSA only requires protection from modification.

FDP_ACC.1.1/Privileged User Creation (the Privileged User is created during TOE initialization only) and FDP_ACC.1/Supply DTBS/R (TOE does not provide facilities for Privileged User to supply the DTBS/R) are trivially satisfied.

FTP_TRP.1/SIC Inter-TSF Trusted path

FTP_TRP.1.1/SIC: The TSF shall provide a communication path between itself and ***Remote Signer through the SIC***[196] users that is logically distinct from other communication paths and provides ensured identification of its end points and protection of the communicated data from *modification*[197].

FTP_TRP.1.2/SIC: The TSF shall permit ***Remote Signer through SIC***[198] to initiate communication via the trusted path.

FTP_TRP.1.3/SIC: The TSF shall require the use of the trusted path for*:*

1) *FDP_ACC.1/Signer Maintenance,*

2) *FDP_ACC.1/Signer Key Pair Generation,*

3) *FDP_ACC.1/Signer Key Pair Deletion,*

4) *FDP_ACC.1/Signing,*

5) *None*[199].

Application Note 83 (Application Note 74 from [4], refined by ST author)

Since it is not all data transmitted to the TOE that needs to be protected in confidentiality, FTP_TRP.1.1/SIC only requires protection from modification.

The only confidential data transmitted in SAP is R.Authorization_Data. This data are encrypted with TOE public key (i.e. infrastructure key), see sec. 1.4 TOE Overview.

FTP_ITC.1/CM - Inter-TSF trusted channel

FTP_ITC.1.1/CM: The TSF shall provide a communication path between itself and **a cryptographic module certified according to EN 419 221-5 [3]** [200] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure

FTP_ITC.1.2/CM: The TSF shall permit **the TSF and a cryptographic module certified according to EN 419 221-5 [3]**[201], to initiate communication via the trusted channel.

[195] [selection: initial user authentication [assignment: other services for which trusted path is required]]
[196] [selection: remote, local]
[197] [selection: modification, disclosure [assignment: other types of integrity or confidentiality violation]].
[198] [selection: the TSF, local users, remote users]
[199] [selection: initial user authentication, [assignment: other services for which trusted path is required]]
[200] refinement (was: “another trusted IT product”)
[201] [selection: the TSF, another trusted IT product]

FTP_ITC.1.3/CM: The TSF shall initiate communication via the trusted channel for *all functions which need a CM (signature validation, signature generation, integrity protection, encryption, decryption, random number generation, cryptographic key generation and destruction)*[202].

Application Note 84 (Application Note 75 from [4], refined by ST author)

The TOE and the CM are located in the same hardware appliance, in the protected environment

6.5. Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5. The assurance components are identified in the table below with the augmented item in bold.

Since the TOE is operated in a physically protected environment as described in OE.ENV an evaluation against this ST will probably not include physical attacks.

Assurance Class	Assurance Components
Development (ADV)	Security architecture description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.4)
	Implementation representation of the TSF (ADV_IMP.1)
	Basic modular design (ADV_TDS.3)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)

[202] [assignment: list of functions for which a trusted channel is required]

	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability assessment (AVA)	**Advanced methodical vulnerability analysis (AVA_VAN.5)**

Table 6.4. Security Assurance Requirements

7. Rationale

7.1. Security Requirements Rationale - Coverage

The following table is used to demonstrate that every SFR is used to cover an objective and that every objective is covered by an SFR. The table is not complete in the sense that all possible crosses are created.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	User Management	OT.PRIVILEGED_USER_MANAGEME NT	OT.PRIVILEGED_USER_AUTHENTICA TION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
Security Audit																					
FAU_GEN.1																					X
FAU_GEN.2																					X
Cryptographic Support																					
FCS_CKM.1/*				X													X				
FCS_CKM.4				X																	
FCS_COP.1/*				X												X	X				
FCS_RNG.1				X															X		
User Data Protection																					
FDP_ACC.1/ Privileged User Creation							X														
FDP_ACF.1/ Privileged User Creation							X														
FDP_ACC.1/ Signer Creation			X							X											
FDP_ACF.1/ Signer Creation			X							X											
FDP_ACC.1/ Signer Maintenance			X							X											
FDP_ACF.1/ Signer Maintenance			X							X											
FDP_ACC.1/ Signer Key Pair Generation				X	X																

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	User Management	OT.PRIVILEGED_USER_MANAGEME NT	OT.PRIVILEGED_USER_AUTHENTICA TION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
FDP_ACF.1/ Signer Key Pair Generation				X	X																
FDP_ACC.1/ Signer Key Pair Deletion										X											
FDP_ACF.1/ Signer Key Pair Deletion										X											
FDP_ACC.1/ Supply DTBS/R															X						
FDP_ACF.1/ Supply DTBS/R															X						
FDP_ACC.1/ Signing												X				X					
FDP_ACF.1/ Signing												X				X					
FDP_ACC.1/ TOE Maintenance																				X	
FDP_ACF.1/ TOE Maintenance																				X	
FDP_ETC.2/ Signer		X																			
FDP_IFC.1/ Signer		X																			
FDP_IFF.1/ Signer		X																			
FDP_ETC.2/ Privileged User							X		X												
FDP_IFC.1/ Privileged User							X		X												
FDP_IFF.1/ Privileged User							X		X												

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	User Management	OT.PRIVILEGED_USER_MANAGEME NT	OT.PRIVILEGED_USER_AUTHENTICA TION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
FDP_ITC.2/ Signer		X																			
FDP_ITC.2/ Privileged User							X		X												
FDP_UCT.1		X																			
FDP_UIT.1		X																			
Identification & Authentication																					
FIA_AFL.1								X				X									
FIA_ATD.1		X					X		X												
FIA_UAU.1								X				X									
FIA_UAU.5/ Signer												X									
FIA_UAU.5/ Privileged User								X													
FIA_UID.2							X		X	X											
FIA_USB.1		X		X			X		X												
Security Management																					
FMT_MSA.1/ Signer										X											
FMT_MSA.1/ Privileged User							X			X											
FMT_MSA.2							X			X											
FMT_MSA.3/ Signer										X											

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	User Management	OT.PRIVILEGED_USER_MANAGEME NT	OT.PRIVILEGED_USER_AUTHENTICA TION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
FMT_MSA.3/ Privileged User							X			X											
FMT_MTD.1																				X	
FMT_SMF.1																				X	
FMT_SMR.2																				X	
Protection of the TSF																					
FPT_PHP.1																				X	
FPT_PHP.3																				X	
FPT_RPL.1													X								
FPT_STM.1																					X
FPT_TDC.1		X					X		X												
Trusted Path/Channels																					
FTP_TRP.1/ SSA															X					X	
FTP_TRP.1/ SIC													X	X	X						
FTP_ITC.1/ CM				X												X					

Table 7.1. Security requirement coverage

7.1.1. Enrolment

OT.SIGNER_PROTECTION is handled by requirements export and import of R.Signer in a secure way (FDP_ETC.2/Signer, FDP_IFC.1/Signer, FDP_IFF.1/Signer, FDP_ITC.2/Signer, FDP_UCT.1, FDP_UIT.1 and FPT_TDC.1). The actual description of the data are described in FIA_ATD.1 and FIA_USB.1.

OT.REFERENCE_SIGNER_AUTHENTICATION_Data are handled by FDP_ACC.1/Signer Creation and FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance and FDP_ACF.1/Signer Maintenance, which describes access control for creating and updating R.Signer and R.Reference_Signer_Authenticaton_Data.

OT.SIGNER_KEY_PAIR_GENERATION is handled by the requirements for key generation and cryptographic algorithms in FCS_CKM.1/* and FCS_COP.1/*. FCS_RNG.1 provides a random source for key generation. FCS_CKM.4 describes the requirements for key destruction. FDP_ACC.1/Signer Key Pair Generation and FDP_ACF.1/Signer Key Pair Generation describes access control for creating a key pair. FIA_USB.1 describes that R.Signing_Key_Id is associated with Signer. FTP_ITC.1/CM can be used to communicate securely with a CM.

OT.SVD is handled by the requirements in FDP_ACC.1/Signer Key Pair Generation and FDP_ACF.1/Signer Key Pair Generation.

7.1.2. User Management

OT.PRIVILEGED_USER_MANAGEMENT is handled by requirements for export and import of R.Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/privileged User, FDP_TC.2/Privileged User and FPT_TDC.1). The actual description of the data are described in FIA_ATD.1 and FIA_USB.1. Authentication of Privileged User is handled by FIA_UID.2, FMT_MSA.1/Privileged User, FMT_MSA.2 and FMT_MSA.3/Privileged User. FDP_ACC.1/Privileged User Creation and FDP_ACF.1/Privileged User Creation describes access controls for creating Privileged Users.

OT.PRIVILEGED_USER_AUTHENTICATION is handled by FIA_AFL.1, FIA_UAU.1 and FIA_UAU.5/Privileged User.

OT.PRIVILEGED_USER_PROTECTION is handled by requirements for export and import of Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/Privileged User, FDP_ITC.2/Privileged User and FPT_TDC.1). The actual description of the data is described in FIA_ATD.1and FIA_USB.1. FIA_UID.2 ensures that Privileged Users are authenticated they can carry out any operation.

OT.SIGNER_MANAGEMENT is handled by the requirements for access control in FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Key Pair Deletion, FDP_ACF.1/ Signer Key Pair Deletion, FDP_ACC.1/ Signer Maintenance and FDP_ACF.1/ Signer Maintenance. Authentication of Signers and Privileged Users are handled by FIA_UID.2, FMT_MSA.1/Signer, FMT_MSA.1/Privileged User, FMT_MSA.2, FMT_MSA.3/Signer and FMT_MSA.3/Privileged User.

7.1.3. Usage

OT.SAD_VERIFICATION is handled by the FIA_AFL.1, FIA_UAU.1 and FIA_UAU.5/Signer. FDP_ACC.1/Signing and FDP_ACF.1/Signing describes access control rules for the signature operation and well as for SAP verification.

OT.SAP is covered by the requirements FTP_TRP.1/SIC and FPT_RPL.1 the protocol between the SIC and TSF.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION is covered by FTP_TRP.1/SIC, which describes the requirements for data transmitted to the TOE, is protected in integrity.

OT.DTBSR_INTEGRITY is covered by FT_TRP.1/SSA and FTP_TRP.1/SIC requiring data transmission to be protected in integrity. Also handled by access control rules FDP_ACC.1/Supply DTBS/R and FDP_ACF.1/Supply DTBS/R for transmitting DTBS/R to the TSF.

OT.SIGNATURE_INTEGRITY is handled by FCS_COP.1/*, which describes requirements on the algorithms. FTP_ITC.1/CM may be used to transmit data securely between the TOE and the CM. Access control for the signature operation is ensured by FDP_ACC.1/Signing and FDP_ACF.1/Signing.

OT.CRYPTO is covered by FCS_CKM.1/* and FCS_COP.1/*, which describes requirements for key generation and algorithms.

7.1.4. System

OT.RANDOM is handled by FCS_RNG.1, which describes requirement on the random number generation.

OT.SYSTEM_PROTECTION is handled by FMT_MTD.1, FMT_SMF.1 and FMT_SMR.2. FDP_ACC.1/TOE Maintenance and FDP_ACF.1/TOE Maintenance describes access control rules for managing TSF data.

FPT_PHP.1 and FPT_PHP.3 describes requirements for TSF protection. FTP_TRP.1/SSA describes that only a Privileged User can maintain the TOE.

OT.AUDIT_PROTECTION is handled by the requirements for audit record generation FAU_GEN.1 and FAU_GEN.2 using reliable time stamps in FPT_STM.1.

7.2. SFR Dependencies

7.2.1. General

The dependencies between SFRs are addressed as shown in Table 7.2.

Requirement	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2 (hierarchical to FIA_UID.1)
FCS_CKM.1/*	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.1/RSA fulfilled by FCS_COP.1/Signature Generation RSA, FCS_COP.1/Signature Verification RSA and FCS_CKM.4 FCS_CKM.1/AES fulfilled by FCS_COP.1/Encryption Decryption and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/*
FCS_COP.1/*	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_COP.1/Signature Generation RSA and FCS_COP.1/Signature Verification RSA fulfilled by FCS_CKM.1/RSA and FCS_CKM.4 FCS_COP.1/Encryption Decryption fulfilled by FCS_CKM.1/AES and FCS_CKM.4 FCS_COP.1/ Message Digest - the dependencies are not necessary because the requirement does not use cryptographic keys
FCS_RNG.1	None	Not applicable
FDP_ACC.1/Privileged User Creation	FDP_ACF.1	FDP_ACF.1/Privileged User Creation
FDP_ACC.1/Signer Creation	FDP_ACF.1	FDP_ACF.1/Signer Creation
FDP_ACC.1/Signer Maintenance	FDP_ACF.1	FDP_ACF.1/Signer Maintenance
FDP_ACC.1/Signer Key Pair Generation	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Generation
FDP_ACC.1/Signer Key Pair Deletion	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Deletion
FDP_ACC.1/Supply DTBS/R	FDP_ACF.1	FDP_ACF.1/Supply DTBS/R

Requirement	Dependencies	Fulfilled by
FDP_ACC.1/Signing	FDP_ACF.1	FDP_ACF.1/Signing
FDP_ACC.1/TOE Maintenance	FDP_ACF.1	FDP_ACF.1/TOE Maintenance
FDP_ACF.1/Privileged User Creation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Privileged User Creation FMT_MSA.3/Privileged User Creation
FDP_ACF.1/Signer Creation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Creation FMT_MSA.3/Signer
FDP_ACF.1/Signer Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Maintenance FMT_MSA.3/Signer
FDP_ACF.1/Signer Key Pair Generation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Key Pair Generation FMT_MSA.3/Signer
FDP_ACF.1/Signer Key Pair Deletion	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Key Pair Deletion FMT_MSA.3/Signer
FDP_ACF.1/Supply DTBS/R	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Supply DTBS/R FMT_MSA.3/ Privileged User
FDP_ACF.1/Signing	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signing FMT_MSA.3/Signer
FDP_ACF.1/TOE Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/TOE Maintenance FMT_MSA.3/Privileged User
FDP_ETC.2/Signer	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Signer
FDP_ETC.2/Privileged User	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Privileged User
FDP_IFC.1/Signer	FDP_IFF.1	FDP_IFF.1/Signer
FDP_IFF.1/Signer	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Signer FMT_MSA.3/Signer
FDP_IFC.1/Privileged User	FDP_IFF.1	FDP_IFF.1/Privileged User
FDP_IFF.1/Privileged User	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Privileged User FMT_MSA.3/Privileged User
FDP_ITC.2/Signer	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FTP_TDC.1	FDP_IFC.1/Signer FTP_TRP.1/SSA and FTP_TRP.1/SIC FPT_TDC.1
FDP_ITC.2/Privileged User	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FTP_TDC.1	FDP_IFC.1/Privileged User FTP_TRP.1/SSA FPT_TDC.1

Requirement	Dependencies	Fulfilled by
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_TRP.1/SSA and FTP_TRP.1/SIC FDP_IFC.1/Signer FDP_IFC.1/Privileged User
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FTP_TRP.1/SSA and FTP_TRP.1/SIC
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	Not applicable
FIA_UAU.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UAU.5/Signer	None	Not applicable
FIA_UAU.5/Privileged User	None	Not applicable
FIA_UID.2	None	Not applicable
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1/Signer	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Signer FMT_SMR.2 (hierarchical to FMT_SMR.1) FMT_SMF.1
FMT_MSA.1/Privileged User	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Privileged User FMT_SMR.2 (hierarchical to FMT_SMR.1) FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FMT_MSA.1/Signer FMT_SMR.2 (hierarchical to FMT_SMR.1)
FMT_MSA.3/Signer	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Signer FMT_SMR.2 (hierarchical to FMT_SMR.1)
FMT_MSA.3/Privileged User	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Privileged User FMT_SMR.2
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 (hierarchical to FMT_SMR.1) FMT_SMF.1
FMT_SMF.1	None	Not applicable
FMT_SMR.2	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FPT_PHP.1	None	Not applicable
FPT_PHP.3	None	Not applicable

Requirement	Dependencies	Fulfilled by
FPT_RPL.1	None	Not applicable
FPT_STM.1	None	Not applicable
FPT_TDC.1	None	Not applicable
FTP_TRP.1/SSA	None	Not applicable
FTP_TRP.1/SIC	None	Not applicable
FTP_ITC.1/CM	None	Not applicable

Table 7.2. Dependencies

7.3. Rationales for SARs

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

As the TOE manages signature creation data generation and authorizes it’s use it manages security attributes which can only be ensured by the TOE. While the TOE is assumed to be in a physically protected environment, it is still subject to logical remote attacks and should be evaluated to deal with High attack potential.

EAL4 is therefore augmented with AVA_VAN.5.

8. TOE Summary Specification

To fulfil the security functional requirements (SFRs), the TOE employs a set of security functions described below.

8.1. TOE Security Functions

The following sections describe the security functions related to one of the SFR classes identified in chapter 6.

8.1.1. Security Audit (FAU)

The TOE logs all security relevant events. The security relevant events are all changes to the system that may impact the overall system security and include all operations invoked by the Privileged User (SimplySign SSA) and Signer.

Each log entry contains the date and time of the event (using a reliable timestamp), the type of event, the identity of the entity that initiated the event. Log entries are associated with the user (Privileged_User or Signer) that caused the event and the outcome (success or failure) of the event. The audit trail does not include any data which allow to retrieve sensitive information.

The security functionality described above meets the requirements:

- FAU_GEN.1 & FAU_GEN.2.

8.1.2. Cryptographic Support (FCS)

The generation of signing keys is handled by a CM certified in accordance with EN 419 221-5 [3]. The CM ensures the quality of the key generation processes, which are invoked by the TOE with appropriate parameters such as key type and size. When the cryptographic keys are no longer used, they are destroyed by the method recommended by FIPS 140-2, i.e. by zeroing.

The security functionality described above meets the requirements:

- FCS_CKM.1/* & FCS_CKM.4

The random strings generation relies on the CM and is ensured by CM's hybrid deterministic random number generator that provides binary string generation that meets the requirements of NIST 800-90A.

The security functionality described above meets the requirements:

- FCS_RNG.1

Digital RSA signatures can be generated using a signing key. Several approved versions of the hash (SHA256, SHA384, SHA512) and padding schemes (RSA PKCS#1 and RSA PSS) are available for the generation of digital signatures by Signers.

The security functionality described above meets the requirements:

- FCS_COP.1/*.

8.1.3. User Data Protection (FDP)

8.1.3.1. Access Control

TOE management and maintenance activities are performed using SimplySign SSA after authentication (which occurs during TOE initialization).

a) User creation

In SimplySign, there is only one Privileged User: SimplySign SSA, which is created during TOE initialization. The SimplySign system does not allow the creation of other Privileged Users.

The security functionality described above meets the requirements of:

- FDP_ACC.1/Privileged User Creation & FDP_ACF.1/Privileged User Creation

The Signer creation process is realized by SimplySign SSA that must be authenticated as Privileged User.

The security functionality described above meets the requirements of:

- FDP_ACC/Signer creation & FDP_ACF/Signer Creation

b) Signer Maintenance

Signer maintenance is divided into tasks that can be handled by the Signer and tasks that can be handled by the SimplySign SSA (Privileged User). The Signer can only maintain its own R.Signer object and no other Signers can maintain it.

The security functionality described above meets the requirements:

- FDP_ACC.1/Signer Maintenance & FDP_ACF.1/Signer Maintenance

c) Signer Key Pair Generation

The Signer key pair generation is performed using the CM.

The private key (signing key) is created and encrypted in the certified CM. No other Signer or Privileged User (SimplySign SSA) has access to the Signer's private key.

The public key (R.SVD) is created in the CM and then transferred via the SimplySign SSA to the CA to obtain the signer's public key certificate.

The security functionality described above meets the requirements:

- FDP_ACC.1/Signer Key Pair Generation & FDP_ACF.1/Signer Key Pair Generation

d) Signer Key Pair Deletion

If Signer keys are no longer used, or if the Signer and/or Privileged User (SimplySign SSA) requests R.Signing_Key_Id to be deleted, then SimplySign SSA deletes the R.Signing_Key_Id.

The security functionality described above meets the requirements:

- FDP_ACC.1/Signer Key Pair Deletion & FDP_ACF.1/ Signer Key Pair Deletion

e) Signing

In order to sign the document(s), the signing operation must be authorised. Authorisation is handled by the TOE by verification of the SAD and PIN and then activation of signing key within the CM.

The DTBS/R is always supplied to the TOE by the Signer as part of the Signature Activation Protocol. The Privileged User never supplies the DTBS/R prior the signature operation.

The security functionality described above meets the requirements:

- FDP_ACC.1/Signing & FDP_ACF.1/Signing, FDP_ACC.1/Supply DTBS/R & FDP_ACF.1/Supply DTBS/R

f) TOE Maintenance

SimplySign SSA is authorized to maintain the TOE as the only Privileged User. All TOE management and maintenance is handled by SimplySign SSA after its authentication. No other users may maintain the TOE.

The security functionality described above meets the requirements:

- FDP_ACC.1/TOE Maintenance & FDP_ACF.1/ TOE Maintenance

8.1.3.2. Export & Import of user data

The TOE exports the following data related with Signer: Signer public key (R.SVD), the result of the signature operation (R.Signature).

TOE does not export or import Privileged User data.

The security functionality described above meets the requirements:

- FDP_ETC.2/Signer & FDP_ITC.2/Signer, FDP_ETC.2/Privileged User & FDP_ITC.2/Privileged User

8.1.3.3. Information Flow

The information flow is protected: only SimplySign SSA, as Privileged User, can create a new Signer (R.Signer attributes are protected for integrity and confidentiality), and next initiate key pair generation on behalf of the Signer.

Key pair generation for the Signer is done by a certified CM.

After Signer creation, the Signer or the Privileged User (SimplySign SSA), can perform management operations on Signer related data.

The security functionality described above meets the requirements:

- FDP_IFC.1/Signer & FDP_IFF.1/ Signer, and FDP_IFC/Privileged User & FDP_IFF.1/Privileged User

8.1.3.4. Data exchange confidentiality and integrity

During a communication session between the SimplySign SSA and the TOE, an AMQP protocol secured by TLS is used that allows the Signers and the Privileged User to transmit requests to the TOE and receive TOE responses in a manner protected from unauthorized disclosure and manipulation.

The security functionality described above meets the requirements:

- FDP_UCT.1 & FDP_UIT.1

8.1.4. Identification and authentication (FIA)

8.1.4.1. Authentication failure handling

The TOE handles authentication failures in a separate way for each role.

Privileged User: if a SimplySign SSA fails to authenticate during TOE initialization, then the TOE (SimplySign SAM) enter to inactive state and require reinitialization by System Administrator.

The security functionality described above meets the requirements:

- FIA_AFL.1

8.1.4.2. User security attributes

The TOE maintains security attributes of SimplySign SSA (Privileged User) and Signer.

The TOE requires SimplySign SSA to be the only Privileged User. When authenticated, SimplySign SSA is authorized to create a Signer or modify its security attributes. The TOE allows the Signer to modify its own data objects.

Some security attributes such as R.Signing_Key_ID, R.SVD may initially be empty.

The security functionality described above meets the requirements:

- FIA_ATD.1 & FIA_USB.1

8.1.4.3. Timing of Authentication

Each user, SimplySign SSA and Signer, when interacting with the TOE must be unambiguously identified and authenticated before TOE allows any actions on their behalf. The TOE considers the Privileged User to be authenticated when the SimplySign TLS certificate is verified during TOE initialization.

The security functionality described above meets the requirements:

- FIA_UAU.1

8.1.4.4. User authentication mechanisms

All SimplySign SSA activities in TOE must be preceded by successful authentication. To do this, during initialization the TOE initiates communication with the SimplySign SSA using TLS channel with mutual authentication (TOE communication component bases on RabbitMQ platform which has built-in TLS support).

On the other hand, the Signer must be successfully identified and authenticated. The signer is identified by an access token and authenticated by a signed SAD (delegated authentication).

The security functionality described above meets the requirements:

- FIA_UAU.5/Privileged User & FIA_UAU.5/Signer.

8.1.4.5. User identification before any action

TOE does not allow a user (Signer and Privileged User) to perform any action before the user is successfully identified and authenticated.

The security functionality described above meets the requirements:

- FIA_UID.2.

8.1.5. Security Management (FMT)

8.1.5.1. Management of security attributes

TOE security features restrict management of system security attributes and data to SimplySign SSA (Privileged User) and Signer.

For all security attributes listed in FIA_USB.1, only secure values are accepted.

The security functionality described above meets requirements:

- FMT_MSA.1/Signer & FMT_MSA.1/Privileged User & FMT_MSA.2.

8.1.5.2. Static attribute initialisation

When creating a Signer, restrictive default values are assigned to security attributes when appropriate. The TOE allows the Privileged User (SimplySign SSA) to specify alternative initial values to override the default values when creating an object or information.

The security functionality described above meets the requirements:

- FMT_MSA.3/Signer & FMT_MSA.3/Privileged User.

8.1.5.3. Management, specification and restrictions on security data

The TOE distinguish two roles: Privileged User (established and authenticated during TOE initialization) and Signer. Any request to change the system configuration, modify security data, manage Singers, can be executed by Privileged User (SimplySign SSA). The Signer can only manage their own data (changing R.Authorisation_data, R.Authorisation_data2, R.Signing_Key_Id, etc.). All the operations are logged by audit.

The security functionality described above meets the requirements:

- FMT_MTD.1, FMT_SMF.1 & FMT_SMR.2

8.1.6. Protection of the TSF (FPT)

8.1.6.1. Protection to physical attack

The TOE is a software component so as such it does not have measures to provide physical protection. The TOE is deployed as a local application within the same physical appliance (CryptoZone) as the CM, which is certified on EN 419-221-5 [3]. The crucial assets (private keys) are managed by the CM, and so the SFRs FTP_PHP.* relies on the similar SFRs described for the CM, which is certified and has its own tamper protection.

The security functionality described above meets the requirements:

- FPT_PHP.1 & FPT_PHP.3.

8.1.6.3. Replay detection

The signature operation is performed using the SAP protocol that requires SAD data. If the TOE detects that the SAD is being used more than once (using timestamps and Signer's access token), it automatically rejects the signature operation and this information will be recorded in the audit logs. The SAP protocol is protected against replay, bypass and forgery attacks by using timestamps and signature authorization of the Signer.

The security functionality described above meets the requirements:

- FPT_RPL1.

8.1.6.4. Reliable time stamps

The TOE and the SCA signing application are synchronized with a reliable timestamp (the time synchronisation is based on the NTP protocol). If the TOE detects a time deviation, it automatically notifies the System Administrator and suspends its operations, i.e. R.Signer creation, signature creation, etc.

The security functionality described above meets the requirements:

- FPT_STM.1

8.1.6.5. Inter-TSF basic TSF data consistency

Resources retrieved by the TOE from SoftCard Database (R.Signer, R.Reference_Signer_Authentication_Data, R.SVD) are protected in integrity by using functionality provided by CM. Resources received by the TOE from Signer and SimplySign SSA (R.SAD, R.DTBS/R) are protected in integrity by hashing functions and secure communication channel features. The TOE has the ability to consistently interpreted this data.

The security functionality described above meets the requirements:

- FPT_TDC.1.

8.1.7. Trusted Paths/Channels (FTP)

8.1.7.1. Trusted Path between TOE & SimplySign SSA/SIC

The TOE provides a trusted communication path between itself and the Privileged User (SimplySign SSA) that is logically separate from other communication paths and ensures that its endpoints are identified and that the transmitted data is protected from modification. All communication between the TOE and Privileged User requires the use of a trusted path. The trusted path is established as TLS tunnel.

The TOE communicates with the remote Signer (through SIC) via SimplySign SSA, using trusted path established between the TOE and SimplySign SSA. The TOE does not verify the SIC as a communication end-point, but relies on the Signer authentication performed by SimplySign SSA.

The TOE requires a trusted path while initiating communication for the signer to sign a document, generate or delete a key pair, or perform maintenance. R.Authorization_Data transmitted to the TOE must be protected in a confidential manner, and the rest of the data need only be protected from modification.

The security functionality described above meets the requirements:

- FTP_TRP.1/SSA & FTP_TRP.1/SIC

8.1.7.1. Trusted channel between TOE & CM

The TOE provides trusted communication between itself and the CM certified to EN 419221-5 [3]. The CM's communication with the TOE is accomplished using vendor-specific API commands for the certified CM.

The security functionality described above meets the requirements:

- FTP_ITC.1/CM.

Bibliography

1. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
2. EN 419241-1:2017, Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements
3. EN 419221-5:2016, Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services
4. EN 419241-2:2019 Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, February 2019
5. BSI-DSZ-CC-0999-2016 for Red Hat Enterprise Linux Version 7.1from Red Hat
6. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
7. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
8. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
9. ETSI EN 319 411-1 v1.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
10. ETSI EN 319 401 v2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
11. ETSI TS 119 312 v1.4.2 (2022-02) Electronic Signature and Infrastructures (ESU); Cryptographic Suites
12. SOG-IS, Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, version 1.2, 2020
13. COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
14. ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
15. FIPS PUB 140-2, Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, May 25, 2001
16. SP 800-90A Rev. 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
17. ISO/IEC 19790:2012 Information technology – Security techniques – security requirements for cryptographic modules
18. COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
19. nShield Solo XC HSM Security Target, v. 1.0, 25th September 2019
20. Entrust, “nShield® Solo, Solo XC and nShield® Edge – User Guide for Linux”, v. 12.80, Nov. 2021
21. FIPS PUB 186-4, Federal Information Processing Standards, Digital Signature Standard (DSS), July 2013
22. RSA Laboratories, PKCS#1: RSA Encryption Standard, Version v2.2, October 27, 2012