Cryptomathic Signer SAM v. 5.1 Security Target for Utimaco Cryptoserver CP5

Document Version:	5.5
Document ID:	ASE_ST_UTIMACO
Date:	March 12, 2020

Document Identification

Document Title:	Cryptomathic Signer Security Target for Utimaco Cryptoserver CP5
Document ID:	ASE_ST_UTIMACO
Document Version:	5.5
Date of version:	March 12, 2020
Origin:	Cryptomathic
Author:	Lone Asferg Laursen, Thomas Brochmann Pedersen
TOE Reference:	Cryptomathic Signer SAM v 5.1 for Utimaco Cryptoserver CP5
Product Type:	QSCD

Terms

Term	Meaning
CA	Certification Authority.
CM	Cryptographic Module. Recides within the HSM.
Cryptographic Module	Cryptographic Module certified according to [EN 419 221-5]. Utimaco CryptoServer Se-Series Gen2 CP5, version 5.1.0.0.
DTBS/R	Data To Be Signed Representation. A hash value of the document to be signed.
HSM	Hardware Security Module.
IdP	Identity Provider.
Privileged User	The users who administrate the TOE and the signer users. This is the Common Criteria term for administrator users.
Administrator	The Signer SAM term for a privileged user.
QSCD	Qualified Electronic Signature (or Electronic Seal) Creation Device as defined in [eIDAS].
RA	Registration Authority.
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol. Protocol use to perform the signature operation.
SCA	Signature Creation Application. Application responsible for creating the document to be signed.
SIC	Signer Interaction Component.
Signer User	End user who can sign documents.
Signing key	A cryptographic key used for signing under the sole control of a signer.
Signing key identifier	Unique identifier of a signing key.
SSA	Server Signing Application [EN 419 241-1].
SVD	Signature Validation Data. A certificate that can be used to validate a signature.
TSP	Trusted Service Provider.
TW4S	Trustworthy system supporting server signing [EN 419 241-1].

Table of Contents

1 Introduction

This Security Target describes the security of a software component being part of the Cryptomathic Signer product. The TOE of this ST is the SAM which is loaded as a local application onto an HSM of type Utimaco CryptoServer Se-Series Gen2 CP5, version 5.1.0.0, see [UT_ST]. The document covers a specification of the security objectives and a description of the security functional requirements of the SAM. The specifications are consistent with the Common Criteria for Information Technology Security Evaluation, Version 3.1 release 5, parts 1, 2, and 3.

This section provides document management and overview information required for a security target. Section 1.1 "Security Target Reference" gives labelling and descriptive information necessary for registering the security target. Section 1.2 "TOE Reference" gives labelling and descriptive information for the TOE. Section 1.3 "TOE Overview" summarizes the TOE in a narrative form. Section 1.4 "TOE Description" contains a description of the TOE including the major security features and operating environment.

1.1 Security Target Reference

Cryptomathic Signer SAM v. 5.1 Security Target for Utimaco Cryptoserver CP5, version 5.3, by Cryptomathic Certification Team, 29 january 2020. CC version 3.1 release 5, see [CC1], [CC2], and [CC3].

1.2 TOE Reference

Cryptomathic Signer SAM version 5.1 for Utimaco Cryptoserver CP5.

Assurance Level: EAL4 augmented with AVA_VAN.5.

1.3 TOE Overview

1.3.1 Purpose and Usage

Cryptomathic Signer is a trustworthy system that offers remote digital signatures as a service. It ensures that the signing key(s) of a signer user are only used under the sole control of the signer user for the intended purpose.

The TOE provides a remote service to the signer user from which he can obtain digital signatures. The functionality and security features of the TOE are centered around protecting this operation, the signer users, and the keys used for the signature generation.

1.3.2 Security Features

The system uses a Cryptographic Module (CM) to generate signing keys and create digital signature values. The Cryptographic Module is an HSM providing the needed cryptographic functionality. The TOE is a software component loaded onto the HSM and it provides the necessary functionality for protecting the attributes of the signer user needed to generate a secure digital signature.

To provide a secure signature service for the signer users, the TOE is able to authenticate the signer users and associate them with signing keys. These keys are protected such that no one but the signer user himself can gain control over his signature key(s). The TOE also provides the means for communication between the signer user and TOE which is protected from modification and disclosure.

Privileged users (administrators in the Signer SAM) are employed for providing the functionality to administrate the signer users and the security configuration of the system. To ensure the secure administration of the TOE, the TOE is also able to authenticate the administrators and provide access only to operations that they are authorized to perform.

Administrators are divided by a role to indicate which tasks they can perform:

- **Security Officer**: Management of TOE and administrators.
- **User Manager**: Management of signer users and signer user key pairs.

1.3.3 TOE Type

The TOE is a software component deployed within the tamper protected part of the Cryptographic Module. Together the TOE and Cryptographic Module are a QSCD.

The TOE implements the Signature Activation Protocol (SAP). The TOE uses the Signature Activation Data (SAD) from the signer user to activate the corresponding signing key for use in a Cryptographic Module.

1.3.4 Usage and Major Security Features of the TOE

The major usage and security features of the TOE are:

- TOE initialization
  - The TOE provides a command for initialization and creation of initial privileged users.
- Operator management
  - Security Officers can create other privileged users.
- System management
  - Security Officers can handle system configuration.
- Signer user management
  - User Managers can create signer users.
  - User Managers or signer users can generate signing keys and Signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a signer user.
- Signature operation
  - Signer users can supply a document to be signed.
  - The link between signer authentication, DTBS/R and signing key identifier is handled by the Signature Activation Data (SAD). This SAD is securely exchanged with the TOE using the Signature Activation Protocol (SAP). Within the TOE the following actions are performed:
    - The SAD is verified in integrity.
    - The SAD is verified that it binds together the signer user authentication, a DTBS/R(s) and signing key identifier.
    - The signer user identified in the SAD is authenticated.
    - The DTBS/R(s) used for signature operations is bound to the SAD.
    - The signing key identifier is assigned to the signer user.
    - The TOE uses Authorisation Data to activate the signing key within the Cryptographic Module.
    - The TOE uses the Cryptographic Module to create signatures.
- An audit trail is produced of all security relevant events within the TOE. Management access to audit trail is outside the scope of the TOE.

The TOE handles data assets as specified in 3.1.

1.3.5 TOE Life Cycle

The TOE life cycle consists of successive phase for development, production, preparation and operational use.

Development: The TOE developer develops the TOE application and its guidance documentation using any appropriate guidance documentation for components working with the TOE, including the Cryptographic Module.

Delivery: The TOE is securely delivered from the TOE developer to the TSP.

Installation and configuration: The TSP installs and configures the TOE with the appropriate configuration and initialization data. Initialization allows creating the initial Security Officers.

Operational phase: In operation, the TOE can be used by Privileged users to create Privileged users and signer users. Privileged users can maintain TOE configuration. Privileged users and signer users may generate signature keys for a signer user. Signer users can supply the data to be signed to the TOE, and authorize a signature creation.

The TOE end of life is out of the scope of this document.

1.3.6 Environment of the TOE

The TOE and Cryptographic Module certified against [EN 419 221-5] is required to obtain a QSCD. Figure 1 gives an overview of the environment in which the TOE is placed. The CM functionality is provided by the HSM including signing key generation and signature operations. The TOE is the SAM software component placed within the HSM. The remaining blue components are parts of the Cryptomathic Signer system. The green components are external components needed for the user to interact with the system.

The signer user is in a local environment and interacts with the Server Signing Application (SSA) in the remote environment to utilize the SSAs signing service. The signature operation is performed using a Signature Activation Protocol (SAP), which requires that Signature Activation Data (SAD) be provided at the local environment. The SAD binds together three elements: signer user authentication with the signing key and the data to be signed (DTBS/R(s)).

To ensure the signer user has sole control of his signing keys, the signature operation needs to be authorized. This is carried out by the TOE, which can handle one endpoint of SAP, verify SAD and activate the signing key within a Cryptographic Module. The Cryptographic Module and the TOE are located within a tamper protected environment. SAD verification means that the TOE checks the binding between the three SAD elements as well as checking that the signer is authenticated.

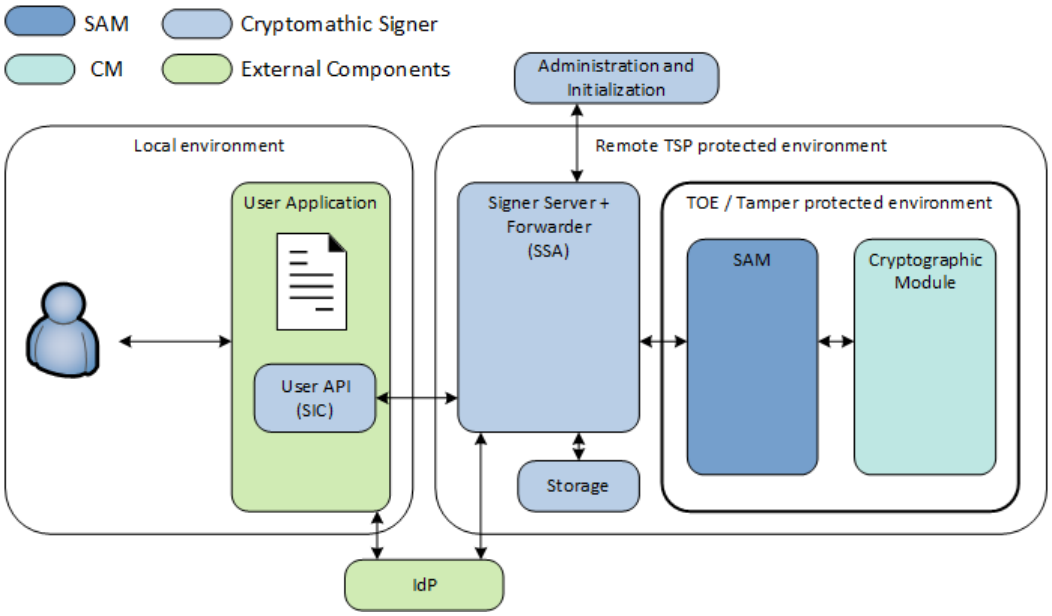


Figure 1: TOE Overview

The signer user authentication is conducted according to [EN 419 241-1] SCAL.2 for qualified signatures. The authentication is done indirectly by the TOE by delegating it to an external authentication service or identity provider (IdP) for strong authentication of the signer users. The authentication service verifies the authentication factor(s) of the signer user and issues an assertion that the signer user has been authenticated. The TOE verifies the assertion.

Since the signer user authentication is not performed directly by the TOE, it has to assume (on the environment) authentication has taken place and rely on assertions. In this document, *signer user authentication* means that the signer has been authenticated using an assertion.

The signer user uses an API acting as signer interaction component (SIC) to communicate with the SSA. The SSA forwards the communication from the SIC to the QSCD. Inside the QSCD the TOE receives the messages and optionally communicates with the SSA to obtain relevant data. When the TOE has verified the SAD, it can authorize the activation of the signing key within the Cryptographic Module and produce a digital signature value. The value is returned to the SSA and may be further delivered to the SCA or SIC. The TOE generates audit records and relies on the SSA to store these records.

Initialization and administration of the system can be done by administrators though the initialization and administration components (administration APIs) provided with the system, see Figure 1.

Administrators need a key pair for authentication purposes. The private key must be stored in a secure way and the administrator authenticates himself to gain access to the private key. The private key is used for signing administrative commands and thus, the TOE holds the public key to be able to verify these signatures. Signature verification indirectly authenticates the privileged user. In this document, *administrator authentication* or *privileged user authentication* means that the administrator has gained access to his private and the TOE has validated his signature on a command.

The system relies on other services (external components in the Figure 1):

- Signer users must be identified and registered. It involves establishment of an authentication mechanism for a signer user. This is provided by the IdP as seen on the Figure 1.
- The user application is responsible for creating the signed document using the signature values provided by the TOE.

To set up the system, the Signer Server (SSA) must be installed as described in the provided documentation and connected to the TOE in the HSM to perform any operations. A forwarding component must also be installed to enable the User SDKs (SIC) to communicate with the SSA. The Initialization Client provided for system initialization must be run before any usage of the system is allowed. External storage must be available for offloading data.

Administration of the system is done by security officers. The Administration Client provided for administration purposes works through the Administration API. Signer users can be created and maintained by user managers. The Administration SDK is provided to the user managers for the purpose of signer user creation and maintenance.

The SIC interface will be installed or loaded on the client machine and then connected to the SSA.

1.3.7 Available non-TOE Hardware/Software/Firmware

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

- A Signature Creation Application (SCA) that manages the document to be signed and transfers that to the SSA, either directly or through the SIC.
- An SSA component which in this solution is the Cryptomathic Signer Server. This component forwards communication between the SIC or administration APIs and the SAM in the QSCD.
- An external storage to persist data.
- A SIC used locally by the signer to communicate with the remote systems. User SDKs are provided for carrying out the SIC responsibilities.
- ~~A Cryptographic Module certified against [EN 419 221-5], which supports the operation of the TOE and performs cryptographic operations. The TOE must be deployed within the same physical boundaries as the Cryptographic Module.~~
- Smart cards and/or key store for administrators to store their authorization data.
- A reliable time source.

These components are delivered wit the Cryptomathic Signer Solution to provide the major non-TOE parts and the guidance to set up the TOE environment:

- The SSA: Cryptomathic Signer Server.
- The SIC either as Java or JavaScript:
  - Cryptomathic Signer User SDK.
  - Cryptomathic Signer JavaScript User SDK.
- Initialization and Administration tools:
  - Cryptomathic Signer Administration Client.
  - Cryptomathic Signer Initialization Client.
  - Cryptomathic Signer Admin SDK.
- From the Cryptomathic Signer General Documentation package:
  - Cryptomathic Signer Installation, Configuration, and Maintenance
  - Cryptomathic Signer Administrators' Manual

The components listed above must be from Cryptomathic Signer 5.1 or later to be compatible with the TOE.

1.4 TOE Description

Cryptomathic Signer enables authenticated users to create digital signatures. Thanks to secure protocols, the protection of a tamper evident environment, and the strict administration procedures enforced by the trust service providers operating the service, it is possible to provide an electronic signature service to key owners.

Cryptomathic Signer offers remote signing using an HSM containing the Cryptographic module and which, when operated according to guidelines, provides a tamper protected environment. The TOE is the software component (SAM) loaded as a local application onto the protected environment of the HSM. It is created to be responsible for all logic performed and for making the final access decisions about whether to allow the usage of a given signing key.

1.4.1 Physical Scope

The TOE is the SAM software component and is loaded onto an HSM which is tamper protected. The HSM is installed with firmware which comprises the Cryptographic Module functionality.

The SAM is retrieved through a download area requiring customer credentials.

The TOE is the following component delivered as an MCT file signed by Utimaco:

Cryptomathic Signer SAM for Utimaco, version 5.1 to be loaded onto an HSM from the Utimaco CryptoServer Se-Series Gen2 CP5, version 5.1.0.0. The Utimaco HSM can be one of the following:

- CryptoServer CP5 Se12 5.1.0.0
- CryptoServer CP5 Se52 5.1.0.0
- CryptoServer CP5 Se500 5.1.0.0
- CryptoServer CP5 Se1500 5.1.0.0.

The following guidance components are needed for CC compliant TOE setup:

- Cryptomathic Signer SAM CC Guidance: AGD-PRE, version 2.0, delivered as PDF file.
- Cryptomathic Signer SAM CC Guidance: AGD-OPE, version 3.2, delivered as PDF file.
- Cryptomathic Signer 5.1 HSM Environment Requirements, version 2.0, delivered as PDF file.
- Cryptomathic Signer SAM CC Compliant Role Configuration, version 2.0, delivered as text file.
- Cryptomathic HSM Setup and Maintenance with SCE. Utimaco CryptoServer CP5 v1.4, as PDF file.

The guidance documents are also retrieved through the download area.

1.4.2 Logical Scope

When installed and configured, the TOE provides a system for creating digital signatures. This section describes the logical entities needed in the system along with the initialization, administration and general usage of the system.

1.4.2.1 Secure initialization

When the system is installed, it is in an uninitialized state and no operations but the initialization can be performed before the system has been initialized.

When initialization is done using the provided Initialization Client, everything is set up in a single call to the TOE. This will set TOE data in a consistent state and prevent that partial initialization can be used to replace parts of the system. During the initialization process, two to four initial Security Officers are created

representing the initial privileged users of the TOE. It is important to note that all initial Security Officers must be present during initialization in order to ensure dual control. The initialization can only be executed once and will result in an operational system with initial privileged users.

1.4.2.2 Privileged users

Privileged users are the users who administrate the TOE and users. Roles are used to define the types of privileged users in the system. Security Officers are responsible for maintenance and configuration and for creating other privileged users. When initializing the system, two to four initial Security Officers are created. Security Officers are responsible for the creation of other privileged users and for TOE maintenance and configuration. User Managers are responsible for enrolling signer users who are the end users of the system and for the maintenance of these signer users giving them the privileges needed to obtain signing keys.

1.4.2.3 Secure Administration

Once initialized, the TOE can only be modified by the Security Officers, starting with the initial ones who were created in the initialization. Every change made to the system must be signed by one or two Security Officers, depending on command type, for it to be accepted.

When an administration command arrives it is processed by the TOE. The TOE checks that the privileged user signatures on the incoming command are legal signatures and that the privileged users are allowed to execute the command. If all this is satisfied, the command is handled and the result is created. All administration commands are audit logged.

Administrators are authenticated using keys stored on smart cards. These smartcards store a key pair where the private key cannot be exported and the server stores the public key in a secure way.

1.4.2.4 Administrator protocol and tools

Administration of the TOE is done through the administrator protocol. All administrator commands are authenticated with keys e.g. located on smart cards. Communication over the administrator protocol is done through a secure channel to the SSA.

Administration tools are provided, the Administration Client and the Administration SDK, both connecting to the server through the administrator protocol.

The Administration Client is a dedicated application providing a GUI for Security Officers for carrying out system administration and security operations. The operations that can be carried out by the Security Officers include:

- System administration and configuration
- Decide which privileged user commands are enabled and which of them requires dual control
- Decide which signer user operations require 2-factor authentication.
- Creation of new privileged users; Security Officers and User Managers.

The Administration SDK is used by the User Manager for operations regarding users, e.g. enrolment and user management. The Administration SDK verifies that the SSA it connects to is trusted using a certificate generated by the SSA and it signs commands with the key belonging to the administrator that wants to connect to the SSA. The Administration SDK can only be used by the User Managers who can use it to create and manage signer users. The operations that can be carried out include:

- Create signer users. The new signer user does not hold any privileges or keys.

- Add a privilege to a user. This results in a key being generated and a certificate request that must be sent to a CA to obtain the certificate which will be added to the signer user.
- Maintain the keys of signer users. Each key is normally associated with a certificate and it is important that the key is renewed when the certificate expires.

Administration of the TOE must follow the guidelines in the guidance documentation provided with the product.

1.4.2.5 Logging and auditing

The TOE provides logs intended for security audit. Two types of events are logged and can be audited; security events and user events.

The security events logged comprises all changes to the system that may impact the overall system security. The log contains all changes to the system that have been invoked though the Administration Client. These log events contains the security critical operations of the TOE and therefore it is the most protected log events. Each entry is protected to prevent changes and the entries are chained to prevent removal of entries.

The user events logged are operations that are related to specific users and thus it allows for auditing a specific user. The log contains operations done using the Administration SDK and SIC including privilege assignment, logons, escalation to two-factor and signing.

1.4.2.6 Signer Users; creation and signing key assignment

Signer users are created by privileged users with the user manager role. When a signer user is created in Signer, he does not have any signing keys. To get a key, the user must be assigned a privilege which allows him to be assigned a signing key with specific properties. Signing keys are always generated by the Cryptographic Module and access to the key is controlled by the TOE. User data and signing keys are stored confidentially and integrity protected in an external storage.

1.4.2.7 Signing key activation

The approach of the TOE is to centralize the storage and management of private signing keys at highly secure environments to keep them logically and physically protected.

To activate a signing key in the TOE, the signer user will need to be authenticated with two factors by one or more external identity providers (IdPs). Before the user sends a signing request to the TOE, he must present assertions from the IdPs in order to retain remote control over his signing key. This means that the user achieves sole control over his private signing key – it cannot be used by any other signer user or by any privileged user.

1.4.2.8 Signature protocol, SAP, and tools

The Signature Protocol is employed to ensure the security of the signing user operations. This protocol together with the security of initialization and secure administration of the system provide the user sole control of keys. The protocol is used to establish confidentiality and integrity protected communication between the SIC and the TOE. The protocol aim to authenticate users and provide access to the signing key.

The SAP – Signature Activation Protocol is used for commencing a signing operation. To gain authorization to use a key the user must set up an authenticated connection. If the authentication is successful, then the user will be able to create a signature using the private signing key. Only on successful authentication will the SAD be available to the signer user. The DTBS/R must be fixed by the IdP when issuing the authorization statement. The DTBS/R can cover multiple documents to be signed.

User operations are carried out through the SIC which relies on the different methods of authentication of the signer users described above. The SIC provides operations for management, authentication, and signing among others, depending on the chosen IdP. Management operations include activation of R.Signer, requesting of a new key, and setting certificate.

2 Conformance Claims

2.1 CC Conformance Claim

This security target is conformant to Common Criteria version 3.1 revision 5.

More precisely, this security target is:

- CC Part 1 [CC1],
- CC Part 2 extended [CC2],
- CC Part 3 conformant [CC3].

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 is conforming to the following protection profile:

- Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing [EN 419 241-2]

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 Cryptographic Module. The TOE uses the asset R.Signing_Key_Id, which identifies a signing key in the Cryptographic Module. The binding of the R.Signing_Key_Id with R.Signer shall be protected in integrity.

Application Note 1

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 Cryptographic Module. The TOE shall ensure that only the signer can use the signing key under his sole control.

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

Application Note 2

The R.Authorisation_Data is used by the Cryptographic Module to activate a signing key. The data may be an asset of the TOE or derived by the TOE from the SAD. In both cases, the TOE must verify the SAD before the R.Authorisation_Data is used to activate the signing key in the Cryptographic Module.

If the TOE derives the R.Authorisation_Data from SAD then this data may not be held by the TOE.

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 Cryptographic Module for signing key pair generation. As part of the signing key pair generation, Cryptographic Module 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.

R.DTBS/R: set of data which is transmitted to the TOE for digital signature creation on behalf of the signer. The DTBS/R(s) is transmitted to the TOE. The R.DTBS/R shall be protected in integrity. The transmission of the DTBS/R(s) to the TOE shall require the sending party - Signer ~~or Privileged User~~ - to be authenticated.

Application Note 3

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

R.SAD: signature activation data is a set of data involved in the signature activation protocol, which activates the signature creation data to create a digital signature under the signer's sole control. The R.SAD must combine:

- The signer's strong authentication as specified in [EN 419 241-1]

- 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 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 5

The unique reference to R.Signing_Key_Id in the R.SAD could be a certificate, a key identifier or derived information obtained from the signer's authentication.

Some solutions may use one-time signing keys, which are generated, certified and used within a limited signing session. The derived information from the signer's authentication may be used to provide session separation if a signer has multiple simultaneous signing sessions with the TOE, or to derive an R.Signing_Key_Id if the key is a one-time key. At the end of the session, the signing key is reliably deactivated.

For solutions that only handle one signing key for each signer, the reference to the R.Signing_Key_Id may also be implied and omitted from the SAD.

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 Cryptographic Module 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 6

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 7

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

R.Reference_Signer_Authentication_Data: is the set of data used by TOE to authenticate the signer. It contains all the data (e.g. OTP device serial number, phone numbers, protocol settings etc.) and keys (e.g. device keys, verification keys etc.) used by the TOE to authenticate the signer. This may include an SVD or certificate to verify an assertion provided as a result of delegated authentication.

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

Application Note 8

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 Cryptographic Module.

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

Application Note 9

The TOE configuration data could include cryptographic algorithm, key length, flows for SAP etc.

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.

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 he provides the SAD and can sign DTBS/R(s) using his signing key in the Cryptographic Module.
- Privileged User, which performs the administrative functions of the TOE ~~and is able to provide a DTBS/R(s) to the TOE as part of the signature operation~~.

Application Note 10

The creation of signers, management of reference signer authentication data and signing key generation is expected to be carried out together with a registration authority (RA) providing a registration service using the SSA, as specified in e.g. [ETSI EN 319 411-1].

3.3 Threats

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.

3.3.1 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 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 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 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 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] clause 6.3.3 d) then an attacker can forge signatures masquerading as the signer.

Application Note 11

There should be a secure transport of R.SVD from TOE to RA or CA. The SAM is expected to produce a CSR.

If the registration services of the TSP issuing the certificate requires a “proof of possession or control of the private key” associated with the SVD, as specified in [ETSI EN 319 411-1] clause 6.3.1 a), this threat can be countered without any specific measures within the TOE.

3.3.2 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 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.

3.3.3 Usage

This section describes threats for signature operation including authentication.

T.AUTHENTICATION_SIGNER_IMPERSONATION

An attacker impersonates 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 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 assets R.DTBS/R and R.SAD are threatened.

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 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 12

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

3.3.4 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 and may be able to activate a signing key.

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

Application Note 13

In some applications, it may be sufficient for an attacker with access to R.Authorisation_Data and R.Signing_Key_Id to activate the signing key within the Cryptographic Module. Since the R.Signing_Key_Id is only to be protected in integrity and not in confidentiality, access to R.Authorisation_Data should only be allowed for authorized operators.

T. AUTHORISATION_DATA _DISCLOSE

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

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

T.CONTEXT_ALTERATION

An attacker modifies system configuration R.TSF_DATA to perform an unauthorized 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 Threads and 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 T. 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_DISCLOSE T.DTBSR_FORGERY
	Confidentiality	T.SIGNATURE_REQUEST_DISCLOSE 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

Asset	Security Dimensions	Threats
		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 1 - Relation between Threads and Assets

3.5 Organizational Security Policies

The TOE shall comply with following the 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/authorization 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 14

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

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]. Guidance for how to implement an enrolment and certificate management system in conformance with [eIDAS] are given in e.g. [EN 319 411-1] or for qualified certificate in e.g. [EN 319 411-2].

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 qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in [eIDAS].

A.ACCESS_PROTECTED

It is assumed that the TOE operates in a protected environment that limits physical access to the TOE to authorized 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 authorized 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 15

The TOE stores all assets outside the TOE, protected in integrity and, when needed, confidentiality. Each operation of the TOE accepts assets relevant to the operation and validates the integrity of those assets.

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 must 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 [eIDAS] and audited to be compliant with the requirements for TSP's given by [eIDAS].

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].

4 Security Objectives

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.

4.1 Security Objectives for the TOE

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

4.1.1 Enrolment

OT.SIGNER_PROTECTION

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

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

The TOE shall be able to securely handle signature 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 Cryptographic Module 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.

4.1.2 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 16

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.

4.1.3 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 17

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

OT.SAP

The TOE shall implement the server-side endpoint of a Signature Activation Protocol (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 18

The signer authentication is assumed to be conducted according to [EN 419 241-1] SCAL.2 for qualified signatures. This means signer authentication can be carried out in one of the following ways:

- Directly by the SAM. In this case the SAM verifies the signer's authentication factor(s).
- Indirectly by the SAM. In the case, an external authentication service as part of the TW4S or a delegated party that verifies the signer's authentication factor(s) and issues an assertion that the signer has been authenticated. The SAM shall verify the assertion.
- A combination of the two directly or indirectly schemes.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION

The TOE shall ensure signature authentication data is protected against attacks when transmitted to the TOE which would compromise its use for authentication.

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.

4.1.4 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 authorized by Privileged User and that unauthorized modification can be detected.

OT.AUDIT_PROTECTION

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

4.2 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].

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] 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 [eIDAS], 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 [eIDAS].

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 cryptographic module consistent with the requirement as defined in [EN 419 241-1] SRG_KM.1.1.

The audit of the qualified TSP according to EN 419 241-1 shall provide evidence that any delegated party meets requirements from EN 419 241-1 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]. 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 [eIDAS] and audited to be compliant with the requirements for TSP's given by [eIDAS]. 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 authorized privileged users. The TOE software and hardware environment (including client applications) shall be installed and maintained by 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] 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].

Application Note 19

In the case that the ST is conformant to this PP and to [EN 419 221-5] as written in the PP Claim section, the certification of the ST covers this requirement for the Operational Environment.

Application Note 20

The ST is comformant to the PP [EN 419 241-2], and is is implemented as a local application within the same physical boundary as the cryptographic module defined in [EN 419 221-5]. In consequence, the certification of the ST covers this requirement for the Operational Environment.

OE.TW4S_CONFORMANT

The TOE shall be operated by a qualified TSP in an operating environment conformant with [EN 419 241-1].

4.2.1 Security Problem Definition and Security Objectives

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

TOE Security Objectives and threats.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD
Enrolment					
T.ENROLMENT_SIGNER_IMPERSONATION		X	X		
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		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					
T.SAP_REPLAY					
T.SAD_FORGERY					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
System					
T.AUTHORISATION_DATA_UPDATE					
T.AUTHORISATION_DATA_DISCLOSE					
T.CONTEXT_ALTERATION					
T.AUDIT_ALTERATION					
T.RANDOM					

Table 2

	User Management	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
Enrolment									
T.ENROLMENT_SIGNER_IMPERSONATION					X				
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED									
T.SVD_FORGERY									
Signer Management									
T.ADMIN_IMPERSONATION			X		X				
T.MAINTENANCE_AUTHENTICATION_DISCLOSE									
Usage									
T.AUTHENTICATION_SIGNER_IMPERSONATION									
T.SIGNER_AUTHENTICATION_DATA_MODIFIED									
T.SAP_BYPASS									
T.SAP_REPLAY									
T.SAD_FORGERY									
T.DTBSR_FORGERY									
T.SIGNATURE_FORGERY									
System									
T.PRIVILEGED_USER_INSERTION		X	X						
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION		X	X	X					
T.AUTHORISATION_DATA_UPDATE								X	
T.AUTHORISATION_DATA_DISCLOSE								X	
T.CONTEXT_ALTERATION								X	
T.AUDIT_ALTERATION									X

T.RANDOM							X		

Table 3

	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO
Enrolment							
T.ENROLMENT_SIGNER_IMPERSONATION							
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED							
T.SVD_FORGERY							X
Signer Management							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Usage							
T.AUTHENTICATION_SIGNER_IMPERSONATION		X					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			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							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Table 4

TOE Security Objectives and Organizational Security Policies.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.RANDOM	OT.CRYPTO
OSP.RANDOM						X	
OSP.CRYPTO							X

Table 5

Threats and Security Objectives for the environment.

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Enrolment							
T.ENROLMENT_SIGNER_IMPERSONATION							X
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED			X	X			
T.SVD_FORGERY	X	X					
Signer Management							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Usage							
T.AUTHENTICATION_SIGNER_IMPERSONATION							
T.SIGNER_AUTHENTICATION_DATA_MODIFIED							
T.SAP_BYPASS				X			
T.SAP_REPLAY				X			
T.SAD_FORGERY			X	X			
T.DTBSR_FORGERY				X			
T.SIGNATURE_FORGERY							
System							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Table 6

Security Objectives for the environment and Assumptions and Security Objectives for the environment.

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Organisational Security Policies							
OSP.TSP_AUDITED							X
OSP.RANDOM							
OSP.CRYPTO							
Assumptions							
A.PRIVILEGED_USER							X
A.SIGNER_ENROLMENT					X		
A.SIGNER_AUTHENTICATION_DATA_PROTECTION			X				
A.SIGNATURE_REQUEST_DISCLOSURE				X			
A.SIGNER_DEVICE				X			
A.CA		X					
A.ACCESS_PROTECTED					X		
A.AUTH_DATA				X			
A.TSP_AUDITED					X		
A.SEC_REQ							X

Table 7

4.2.2 Rationale for the Security Objectives

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

4.2.2.1 Threats and 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 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 signer.

It is also covered by OE.TW4S_CONFORMANT as that requiressigner enrolment to be handled in accordance with [Assurance] 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.

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 Cryptographic Module 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 authorized manner.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE is covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring that authentication data be securely handled.

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.

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 must completed.

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

T.SAP_REPLAY is covered by OT.SAP requiring that the signature activation protocol must be able to resist whole or part of it being replayed.

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

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 the in 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 unauthorized modification to TOE configuration to be detectable.

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

T.CONTEXT_ALTERATION is covered by OT.SYSTEM_PROTECTION requiring any unauthorized 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.

4.2.2.2 Organizational security policies and 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 cryptographic module to provide a tamper-protected environment and for cryptographic functionality and random number generation.

4.2.2.3 Assumptions and objectives

A.PRIVILEGED_USER is covered by OE.TW4S_CONFORMANT requiring the TOE's administrator to be 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].

5 Extended Components Definition

5.1 Class FCS: Cryptographic Support

The Class FCS: Cryptographic Support as defined in [CC2] 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:

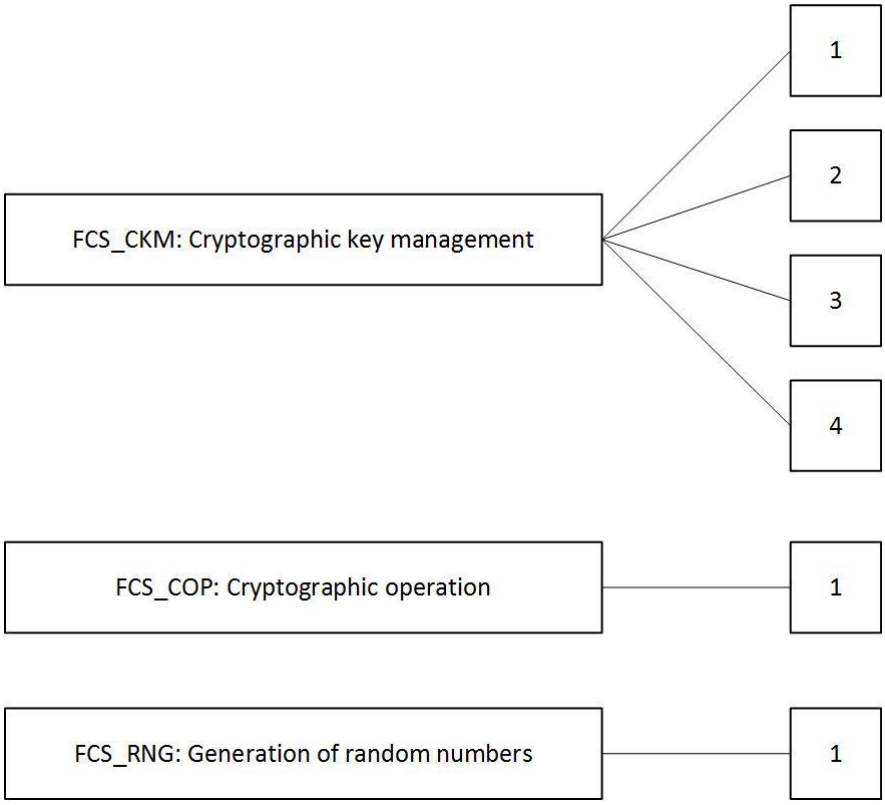


Figure 2

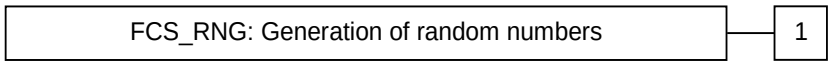
5.1.1 Generation of Random Numbers (FCS_RNG)

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

Family behavior:

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

Component levelling:



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 21

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

6.2 Subjects, Objects and Operations

This section describes the subjects, object 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 for R.Signer

Table 8

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 Cryptographic Module to activate the private part of a R.Signer signature key pair
R.Signature	The result of a signature operation
R.TSF_DATA	TOE Configuration Data

Table 9

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.

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 limits 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 an 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 describes 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_Authenticaton_Datamaintaining 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 an ST specified list of algorithms.

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.

Privileged User Creation

- FDP_ACC.1/Privileged User Creation using FDP_ACF.1/ Privileged User Creation describes access control requirements for creating an 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.

Validate Audit

- FDP_ACF.1/Audit using FDP_ACC.1/Audit describes access control requirements for validating the audit log.

Communication

- FPT_ITC.2 requires that all communication to the TOE comes from the SSA.
- FTP_TRP.1/SSA and FTP_TRP.1/SIC requires that either the Privileged User or the Signer initiates the communication.

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 [selection: *minimum*[1]] 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) [assignment: *None*[2]].

Application Note 22

[1] [selection: minimum, basic, detailed, not specified]

[2] [assignment: other specifically defined auditable events]

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 23

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

Application Note 24

The audit log entries for the signing operation contain the R.DTBS/R.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: Type of action performed (success or failure), identity of the role which performs the operation. [assignment: *none*[3]]]

Application Note 25

Audit trail shall not include any data which allow to retrieve sensitive data like R.SAD, R.Reference_Signer_Authentication_Data and R.Authorisation_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 Cryptographic key generate

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *key generation algorithms listed in Table 10*[4]] and specified cryptographic key sizes [assignment: *key sizes*

[3] [assignment: other audit relevant information]

[4] [assignment: cryptographic key generation algorithm]

listed in Table 10[5]] that meet the following: [assignment: *standards listed in Table 10*[6]].

Key Type	Key Generation Algorithm	Key Size/Curve	Standard
AES	AES key generation	256	[FIPS 197], chapters 3.1 and 6
RSA	RSA key pair generation with pre-defined or given public exponent	2048, 3072, or 4096	[SOGIS], section 4.1
ECC	ECDSA key pair generation with given elliptic curve domain parameters	P-256, P-384, or P-521	[FIPS 186-4], chapter 6
ECC	ECDSA key pair generation with given elliptic curve domain parameters	brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, or brainpoolP512t1	[ECCBP], chapter 10

Table 10: Key Generation Algorithms

Application Note 26

The TOE is expected to use a cryptographic module certified in conformance with [EN 419 221-5], 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 cryptographic module with the appropriate parameters whenever key generation is required.

Guidance on cryptographic algorithms can be found in [ETSI TS 119 312] and [SOGIS].

Application Note 27

The ST is expected to use cryptographic keys for different purposes, e.g. application, infrastructure, session etc. The ST writer should include an iteration of this SFR for every key type (e.g. RSA and AES) it generates itself.

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 [assignment: *zeroization*[7]] that meets the following: [assignment: *None*[8]].

[5] [assignment: cryptographic key sizes]

[6] [assignment: list of standards]

[7] [assignment: cryptographic key destruction method]

[8] [assignment: list of standards]

Application Note 28

The TOE is expected to use a cryptographic module certified in conformance with [EN 419 221-5] for key destruction.

Application Note 29

All cryptographic keys are destroyed by this process[9].

FCS_COP.1	Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *Operations listed in Table 11*[10]] in accordance with a specified cryptographic algorithm [assignment: *Algorithms listed in Table 11*[11]] and cryptographic key sizes [assignment: *Key sizes listed in Table 11*[12]] that meet the following: [assignment: *Standards listed in Table 11*[13]].

Application Note 30

The TOE is expected to use a cryptographic module certified in conformance with [EN 419 221-5] for cryptographic operations.

Application Note 31

The TOE uses the cryptographic module for the cryptographic operations listed in Table 11.

Operation	Key Type	Key Size	Algorithm	Standard
Signature validation	RSA	2048, 3072, or 4096	RSASSA-PKCS1-v1.5 RSASSA-PSS	[PKCS#1] , Chapters 8.1.2 and 8.2.2
Signature generation	RSA	2048, 3072, or 4096	RSASSA-PKCS1-v1.5 RSASSA-PSS	[PKCS#1], Chapters 8.1.1 and 8.2.1
Signature generation	ECC	P-256, P-384, P-521, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1,	ECDSA	[ANSI-X9.62]

[9] The ST writer should include an iteration of this SFR for purposes of keys that it destructs itself

[10] [assignment: list of cryptographic operations]

[11] [assignment: cryptographic algorithm]

[12] [assignment: cryptographic key sizes]

[13] [assignment: list of standards]

		brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, or brainpoolP512t1		
Confidentiality	RSA	2048, 3072, or 4096	RSAES-OAEP	[PKCS#1], Chapter 7.1
	AES	256	AES-CBC	[NIST SP 800-38A], Chapter 6.2
Integrity protection	AES	256	HMAC	[FIPS 198] and [RFC2104]
Integrity and confidentiality protection	AES	256	AES-GCM	[NIST-SP800-38D]
Key derivation	AES	256	KDF in Feedback Mode with HMAC	[NIST SP 800-108], Chapter 5.2

Table 11: Cryptographic Operations

Application Note 32

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 [eIDAS] and a list of approved signature and seal formats are given in [Formats].

Signature Generation Algorithm	Padding	Hash Algorithm
RSA	RSASSA-PKCS1-v1.5 RSASSA-PSS	SHA256 SHA384 SHA512

Table 12: Digital Signature Generation Table

The next SFR is relevant when the TOE is deployed in an appliance distinct form the Cryptographic Module.

FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1	The TSF shall provide a [selection: *hybrid deterministic*[14]] random number generator that implements: [assignment: *list of security capabilities as required by FCS_RNG.1.1 of [UT_ST]*[15]].
FCS_RNG.1.2	The TSF shall provide [selection: *octets of bits*[16]] that meet [assignment: *the quality metric required by FCS_RNG.1.2 of [UT_ST]*[17]].

[14] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

[15] [assignment: list of security capabilities]

[16] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]

[17] [assignment: a defined quality metric]

Application Note 33

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

Application Note 34

The SFR FCS_RNG.1 only apply, if the TOE is not implemented as a local application within the same physical boundary as the cryptographic module – otherwise, the SFRs defined in [EN 419-221-5] already provide requirements on generation of random numbers. This should be stated in the Security Target.

Application Note 35

Since the SAM is implemented as a local application within the same physical boundary as the cryptographic module, FCS_RNG.1 in [UT_ST] provides the requirements for FCS_RNG.1.

6.4.3 User Data Protection (FDP)

Role	Additional Security Attributes	Authorized operations
Security Officer		Privileged User Creation TOE Maintenance
User Manager		Signer Creation Signer Key Pair Generation Signer Maintenance
Signer	Authentication Level=1	Signer Key Pair Generation Signer Maintenance
Signer	Authentication level=2	Signing

Table 13: User Authorization Table

Application Note 36

The User Authorization Table shows which roles are authorized to perform certain operations. Security Officer and User Manager are sub-roles of Privileged User (See FMT_SMR.2).

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* 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.*

Application Note 37

At TOE initialization, 2-4 Privileged Users, with the Security Officer role, are created.

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* to objects based on the following: *(1) whether the subject is a **Security Officer** ~~Privileged User~~ authorized to create a new Privileged User.*
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 **Security Officer** ~~Privileged User~~ who has been authorised for creation of new users can carry out the Create_New_Privileged_User operation.*
FDP_ACF.1.3/ Privileged User Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None.*
FDP_ACF.1.4/ Privileged User Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None.*

FDP_ACC.1/Signer Creation	Subset access control

FDP_ACC.1.1/ Signer Creation	The TSF shall enforce the *Signer Creation SFP* 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*

FDP_ACF.1/Signer Creation	Security attribute based access control

FDP_ACF.1.1/ Signer Creation	The TSF shall enforce the *Signer Creation SFP* to objects based on the following: *(1) whether the subject is a **User Manager** ~~Privileged User~~ authorized to create a new Signer.*
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 **User Manager** ~~Privileged User~~ who has been authorised for creation of new users can carry out the Create_New_Signer operation.*
FDP_ACF.1.3/ Signer Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None.*
FDP_ACF.1.4/ Signer Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None.*

FDP_ACC.1/Signer Maintenance	Subset access control

FDP_ACC.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP*[18] 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*[19]*.*

FDP_ACF.1/Signer Maintenance	Security attribute based access control

FDP_ACF.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP*[20] to objects based on the following: *(1) Whether the subject is a ~~Privileged User or~~ Signer authorised to maintain the Signer security attributes*[21].
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 authorised to maintain a Signer can carry out the Signer_Maintenance operation*[22]*.*
FDP_ACF.1.3/ Signer Maintenance	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 to be maintained*[23]*.*
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*[24]*.*

Application Note 38

Only the Signer can maintain R.Reference_Signer_Authentication_Data belonging to that Signer.

FDP_ACC.1/Signer Key Pair Generation	Subset access control

[18] [assignment: *access control SFP*]

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

[20] [assignment: *access control SFP*]

[21] [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*]

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

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

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

FDP_ACC.1.1/ Signer Key Pair Generation	The TSF shall enforce the *Signer Key Pair Generation SFP*: *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 TOE requests the Cryptographic Module to generate a signing key pair R.Signing_Key_Id and R.SVD and assign them to the R.Signer.*

Application Note 39

R.Authorisation_Data is created by the cryptographic module together with R.Signing_Key_Id and R.SVD, and is kept by the TOE.

Application Note 40

Signing keys can be used by several cryptographic modules, as long as they have been initialized with identical TSF data. Integrity of the key and linking to R.Signer is governed by FPT_TDC and confidentiality by FDP_UCT.

Application Note 41

Signing keys are generated on-demend for a specific user, and so a signing key is always assigned to a Signer.

Application Note 42

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

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* to objects based on the following: *(1) Whether the subject is a **User Manager** ~~Privileged User~~ or Signer authorised to generate a key pair.*
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 **User Manager** ~~Privileged User~~ or Signer who has been authorised to generate the key pair can carry out the Generate_Signer_Key_Pair operation.*
FDP_ACF.1.3/ Signer Key Pair Generation	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 where the key pair is to be generated.*
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.

Application Note 43

The TOE does not provide pre-generated keys.

Application Note 44

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*[25] 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 from R.Signer*[26].~~

Application Note 45

Deletion of R.Signing_Key_Id may also require that the signing key is deleted by the Cryptographic Module.

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

Application Note 46

Application Note 45 implies that the requirement only applies if the delete operation is performed by the TOE. The TOE does not provide any interface for deleting R.Signing_Key_Id and R.SVD of R.Signer, and thus the requirement is not applicable.

~~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*[27] to objects based on the following:~~ ~~*(1) Whether the subject is a Privileged User or Signer authorised to delete the Signer security attributes*[28].~~
~~FDP_ACF.1.2/~~	~~The TSF shall enforce the following rules to determine if an operation among~~

[25] [assignment: *access control SFP*]

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

[27] [assignment: *access control SFP*]

[28] [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*]

~~Signer Key Pair Deletion~~	~~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*[29].~~
~~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*[30].~~
~~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*[31].~~

The PP allows Privileged Users to supply DTBS/R on behalf of the Signer, as expressed by the following SFR. The TOE only allows the DTBS/R(s) to be supplied to the TOE by the Signer as part of the Signature Activation Protocol, which is covered by the FDP_ACC.1/Signing.

~~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* 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.*~~

Application Note 47

The TOE does not provide facilities for Privileged Users to supply the DTBS/R(s), so 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* to objects based on the following:~~ ~~*(1) Whether the subject is a Privileged User authorised to supply a DTBS/R(s).*~~
~~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:~~ ~~*(1) Only a Privileged User who has been authorised to supply a DTBS/R(s)~~

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

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

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

~~*can carry out the Supply_DTBS/R operation.*~~

~~FDP_ACF.1.3/ Supply DTBS/R~~	~~The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None.*~~
~~FDP_ACF.1.4/ Supply DTBS/R~~	~~The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None.*~~

Application Note 48

The TOE does not provide facilities for Privileged Users to supply the DTBS/R(s), so 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* 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.Autorisation_Data and R.Signing_Key_Id to activate a signing key in the Cryptographic Module and signs the R.DTBS/R resulting in R.Signature.* • *The TOE deactivates the signing key when the signature operation is completed.*

Application Note 49

R. Authorisation_Data contains the CM signing key token and R.Signing_Key_Id protected in both integrity and confidentiality. The TSF activates the signing key by decrypting R. Authorisation_Data and loading the CM signing key token into the CM. The TSF will only decrypt R. Authorisation_Data when provided as part of the Signing operation together with the same R.Signing_Key_Id as is contained in R.Authorisation_Data, and when the integrity of R.Authorisation_Data is verified.

Application Note 50

The Signer provides R.DTBS/R(s) as part of the Signing operation.

Application Note 51

Signing key deactivating means that the signer shall authorise 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* to objects based on the following:
(1) Whether the subject is a Signer authorised to create a signature.

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:
(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 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.
(6) [R.Signing_Key_Id is linked to R.Authorisation_Data]

FDP_ACF.1.3/ Signing — 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 used to generate the signature.

FDP_ACF.1.4/ Signing — 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 used to create a signature.

Application Note 52

In FDP_ACF.1.2/Signing the R.Signing_Key_Id can be implied if the signing uses a one-time keys or a signing key is known to be the default.

If the TOE uses configuration data, then the following SFR is used to maintain it.

FDP_ACC.1/TOE Maintenance	Subset access control

FDP_ACC.1.1/ TOE Maintenance — The TSF shall enforce the *TOE Maintenance SFP* on:
Subjects: Privileged User
Objects: R.TSF_DATA.
Operations: TOE_Maintenance:
The Privileged User transmits information to the TOE to manage R.TSF_DATA.

FDP_ACF.1/TOE Maintenance	Security attribute based access control

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

Maintenance	*(1) Whether the subject is a **Security Officer** ~~Privileged User~~ authorised to maintain the TOE configuration data.*
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 **Security Officer** ~~Privileged User~~ who has been authorised to maintain the TOE can carry out the TOE_Maintenance operation.*
FDP_ACF.1.3/ TOE Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None.*
FDP_ACF.1.4/ TOE Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None.*

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* 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.~~
~~FDP_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 is exported from the TSF: *None*.~~

Application Note 53

The TOE does not support export of user data.

FDP_IFC.1/Signer	Subset information flow control

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

FDP_IFF.1/Signer	Simple security attributes

FDP_IFF.1.1/ Signer	The TSF shall enforce the *Signer Flow SFP* based on the following types of subject and information security attributes: **User Manager** ~~*Privileged User*~~ *and Signer accessing the Signer security attributes*.
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 Deletion,~~ FDP_ACC.1/Supply DTBS/R, FDP_ACC.1/Signer Maintenance and FDP_ACC.1/Signing.
FDP_IFF.1.3/ Signer	The TSF shall enforce the: *None*.
FDP_IFF.1.4/ Signer	The TSF shall explicitly authorise an information flow based on the following rules: *None.*
FDP_IFF.1.5/ Signer	The TSF shall explicitly deny an information flow based on the following rules: *None*.

~~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* 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.~~
~~FPP_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 is exported from the TSF: *None*.~~

Application Note 54

The TOE does not support export of user data.

FDP_IFC.1/Privileged User Subset information flow control

FDP_IFC.1.1/ Privileged User	The TSF shall enforce the *Privileged User Flow SFP* on *Privileged User accessing Privileged User security attributes for all operations*.

FDP_IFF.1/Privileged User Simple security attributes

FDP_IFF.1.1/ Privileged User	The TSF shall enforce the *Privileged User Flow SFP* based on the following types of subject and information security attributes: **Security Officer** ~~*Privileged User*~~ *accessing the Privileged User security attributes*.
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.*
FDP_IFF.1.3/ Privileged User	The TSF shall enforce the: *None*.
FDP_IFF.1.4/ Privileged User	The TSF shall explicitly authorise an information flow based on the following rules: *None.*

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

~~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, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP* 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 is 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*.~~

Application Note 55

The TOE does not support import of user data.

~~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* 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 is 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*.~~

Application Note 56

The TOE does not support import of user data.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP*[32] to *transmit and receive*[33] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP*[34] to *transmit and receive*[35] user data in a manner protected from *modification and insertion*[36] errors **for R.Signer and R.Privileged User and for R.SAD also**[37] from *modification and replay*[38] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion and insertion*[39] **for R.Signer and R.Privileged_User and for R.SAD**[40] *whether modification and replay*[41] has occurred.

Application Note 57

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 [selection: [assignment: positive integer number], a TOE Maintenance configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to Privileged User and Signer authentication.~~

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

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

[33] [selection: *transmit, receive*]

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

[35] [selection: *transmit, receive*]

[36] [selection: *modification, deletion, insertion, replay*]

[37] 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.

[38] [selection: *modification, deletion, insertion, replay*]

[39] [selection: *modification, deletion, insertion, replay*]

[40] The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred

[41] [selection: *modification, deletion, insertion, replay*]

Application Note 58

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

Application Note 59

Signers are authenticated by delegated authentication by an IdP. It is the responsibility of the IdP to detect failed authentication and suspend signer users. Privileged users are authenticated when gaining access to their private key. Since the TOE does not support direct authentication, this requirement is not relevant.

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*.

FIA_UAU.1	Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*no action*[42]] on behalf of the user to be performed before the user is authenticated.

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

Application Note 60

The TOE only supports indirect authentification. The TOE consideres a user to be authenticated when an assertion/signature has been validated.

FIA_UAU.5/Signer	Multiple authentication mechanisms

FIA_UAU.5.1/Signer The TSF shall provide [*IdP assertion validation*[43]] to support Signer authentication.

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

- [If Authentication_Level=0, the TSF shall verify the correctness of an assertion to authenticate the Signer and set the Authentication_Level=1 security attribute if the assertion passes. If Authentication_Level=1, and the user authenticates with an additional assertion, the TSF will set the security attribute Authentication_Level=2[44]].

[42] [assignment: list of TSF mediated actions]

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

[44] [selection: [assignment: the rules describing how delegated authentication is verified by the TSF], [assignment: the rules describing how direct authentication mechanisms provide authentication]]

Application Note 61

This SFR only applies to signer authentication for maintaining signer (FDP_ACC.1/Signer Maintenance, **and** FDP_ACC.1/Signer Key Pair Generation ~~and FDP_ACC.1/Signer Key Pair Deletion~~) and for signing (FDP_ACC.1/Signing).

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

FIA_UAU.5/Privileged User	Multiple authentication mechanisms

FIA_UAU.5.1/Privileged User	The TSF shall provide [*signature validation*[45]] to support Privileged User authentication.
FIA_UAU.5.2/Privileged User	The TSF shall authenticate any user's claimed identity according to the [*Verification of signatures on communication with Privileged User*[46]].

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* *(2) R.Signing_Key_Id* *(3) R.SVD* *(4) R.Signer* *(5) [Authentication_Level[47]]* *to Signer* *(1) R.Reference_Privileged_User_Authentication_Data* *(2) [role[48]]* *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:

[45] [assignment: list of authentication mechanisms]

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

[47] [*assignment: list of user security attributes]*

[48] [*assignment: list of user security attributes]*

(1) Whether the subject is a Privileged User authorized to create a new Signer.
(2) *Whether the subject is a Privileged User authorized to create a new Privileged User.*
(3) *[None[49]].*

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[50]].*

Application Note 62

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

Application Note 63

R.Authrorisation_Data is not a security attribute of the Signer.

Application Note 64

R.DTBS/R is not 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 to restrict the ability to create the security attributes listed in FIA_USB.1 for Signer to authorized ***User Managers*** ~~*Privileged User*~~*.*
(2) Generate Signer Key Pair SFP to restrict the ability to generate the security attributes R.SVD and R.Signing_Key_Id to authorized ***User Managers*** ~~*Privileged User*~~ *and Signer.*
(3) ~~*Signer Key Pair Deletion SFP[51] to restrict the ability to destruct[52] the security attribute R.SVD and R.Signing_Key_Id as part of R.Signer[53] to authorised Signer[54]*~~
(4) Supply DTBS/R SFP to restrict the ability to create the security attribute

[49] [*assignment: rules for the initial association of attributes]*

[50] [*assignment: rules for the changing of attributes]*

[51] [assignment: *access control SFP(s), information flow control SFP(s)*]

[52] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[53] [assignment: *list of security attributes*]

[54] [assignment: *the authorised identified roles*]

R.DTBS/R as part of R.Signer to authorized ***User Managers*** ~~*Privileged User*~~*.*

(5) Signing SFP to restrict the ability to create the security attribute R.DTBS/R as part of R.Signer to authorized Signer.

(6) Signing SFP to restrict the ability to query the security attributes as listed in FIA_USB.1 to authorized Signer.

(7) *Signer Maintenance SFP to restrict the ability to change the security attributes R.Reference_Signer_Authentication_Data as part of R.Signer to authorized* ***User Managers*** ~~*Privileged User*~~ *and Signer.*

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 to restrict the ability to create and query the security attributes listed in FIA_USB.1 for Privileged User to authorised ***Security Officer*** ~~*Privileged User*~~*.*

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*.

FMT_MSA.3/Signer	Static attribute initialization

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

FMT_MSA.3.2/ Signer — The TSF shall allow the **User Manager** ~~*Privileged User*~~ to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Privileged User	Static attribute initialization

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

FMT_MSA.3.2/ Privileged User — The TSF shall allow the **Security Officer** ~~*Privileged User*~~ 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

(1) Modify the *R.TSF_DATA* data to **Security Officer** ~~*Privileged User*~~.

Application Note 65

The TSF data includes configuration of 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*[55]].

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: *Signer and Privileged User,* [*Security Officer and User Manager*[56]].
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* are satisfied.

Application Note 66

A user having any of the roles "Security Officer" or "User Manager" automatically has the role Privileged User (See section Application Note 33 for a list of authorized operations).

6.4.6 Protection of the TSF (FPT)

FPT_PHP.1 Passive

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 67

[55] [assignment: additional list of management functions to be provided by the TSF]

[56] [assignment: other authorized identified roles]

Passive detection of a physical attack is typically achieved by using physical seals and an appropriate physical design of the TOE that allows the TOE administrator to verify the physical integrity of the TOE as part of a routine inspection procedure.
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] for Security Level 3.

FPT_PHP.3	Resistance

FPT_PHP.3.1 The TSF shall resist [*physical manipulation*[57]] to the [*cryptographic module*[58]] by responding automatically such that the SFRs are always enforced.

Application Note 68

The TOE is implemented as a local application within the same physical boundary as the cryptographic module defined in [EN 419-221-5], and so the SFRs FTP_PHP.* rely on the similar SFRs described in the ST for the cryptographic module.

Application Note 69

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 zeroisation 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] for Security Level 3.

FPT_RPL.1	Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *R.SAD*.
FPT_RPL.1.2 The TSF shall perform *reject the signature operation* when replay is detected.

~~FPT_STM.1~~	~~Reliable time stamps~~

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

[57] [assignment: *physical tampering scenarios*]

[58] [assignment: *list of TSF devices/elements*]

Application Note 70

The TOE **receives** ~~may receive~~ a reliable time source from its environment.

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*

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* when interpreting the TSF data from another trusted IT product.

Application Note 71

The SFR is used to handle the situation where the whole or part of the above data are stored outside the TOE.

FPT_TDC.1/Audit	Inter-TSF basic TSF data consistency

FPT_TDC.1.1/Audit The TSF shall provide the capability to consistently interpret [R.Audit[59]] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Audit The TSF shall use [*data integrity on data*[60]] when interpreting the TSF data from another trusted IT product.

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 users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the

[59] assignment: list of TSF data types

[60] assignment: list of interpretation rules to be applied by the TSF

communicated data from *modification*.

FTP_TRP.1.2/SSA The TSF shall permit Privileged User through SSA 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
(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*[61]].

Application Note 72

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.

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 users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification*.

FTP_TRP.1.2/SIC The TSF shall permit Remote Signer through SIC 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*[62]].

Application Note 73

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. All data transferred from the Signer to the TOE is protected in confidentiality to protect sensitive data.

The TOE is not expected to verify the SIC as a communication end point and it may rely on the signer authentication.

[61] [assignment: other services for which trusted path is required]

[62] [assignment: other services for which trusted path is required]

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]* that is logically distinct from other communication paths and provides assured authentication 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]* to initiate communication via the trusted channel.

FTP_ITC.1.3/CM The TSF shall initiate communication via the trusted channel for [*signature validation, signature generation, integrity protection, encryption, decryption, random number generation, cryptographic key generation*[63]].

Application Note 74

Since the TOE and the cryptographic module are located within the same hardware appliance the trusted channel is mapped in the Security Target to the physical configuration, and no additional authentication or cryptographic protection are required (because of the physical security assumed in the appliance 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 PP 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)

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

Assurance Class	Assurance Components
	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)
	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 14

7 TOE Summary Specification

The TOE employs a variety of security functionality (TSF) to satisfy the SFRs in order to provide creation of digital signatures. This chapter summarizes the security capabilities of the TOE to clarify the solutions implemented to ensure that the SFRs are satisfied.

Each of the following sections describe the security functionality related to one of the SFR classes identified in chapter 6**.** The sections are when relevant ordered by the functionality provided.

7.1 Security Audit (FAU)

The security functionality described below satisfies FAU_GEN.1 and FAU_GEN.2.

Audit logging is implemented in the TOE, and it recognizes and creates records for all security relevant events and user specific events. The security relevant events are all changes to the system that may impact the overall system security and contains all operations invoked through the Administration Client using the administrator protocol. The user specific events are all operations related to specific users. This allows auditing what has happened to a user account. This contains operations done in the Administration SDK and the SIC. Events logged include usage of the signing key of a signer user and the generation of certification requests instigated by a given privileged user with the user manager role.

Each log entry contains basic information about the event that occurred such as description and time stamp. For relevant events the log entry also includes the DTBS/R. For failure events, the failure is indicated in the log entry. The log entries never contain data that can be used for retrieving sensitive data like R.SAD, R.Authentication_Data, or R.Authorisation_Data.

The identity of the relevant user is included in the log entries when applicable. For privileged users the command signature is verified to determine the relevant user. For signer users the user session of an authenticated user is used for associating a user with a given operation. Each log entry can subsequently be associated to the user (R.Signer or R.Privileged_User) who caused the event except for logs of system events not instigated by a user.

The resulting audit records are stored securely in the external storage and are protected from modification. The audit records for TOE management events are also protected against deletion.

7.2 Cryptographic Support (FCS)

The security functionality described below satisfies FCS_CKM.1 and FCS_CKM.4 regarding cryptographic keys, and FCS_COP.1 regarding cryptographic operation.

7.2.1 Cryptographic Keys

The generation of signing keys is handled by the cryptographic module. Key generation is invoked with appropriate parameters such as key type and size. The usage of a cryptographic module certified in conformance with [EN 419 221-5] ensures the quality of the generated keys. Cryptographic keys are destroyed by zeroisation when they are no longer in use.

7.2.2 Cryptographic Operation

Digital signatures can be generated using a signing key. The user can choose between the approved variations of hash functions and encodings as defined in FCS_COP.1.

7.3 User Data Protection (FDP)

The protection of user data is the most comprehensive part of the security functionality of the TOE. Multiple entities must be protected for the two kinds of users in the system; Signer users and privileged users. Data must be protected through the entire lifecycle from creation over e.g. maintenance, usage, and renewal to the possible destruction if the data is no longer used. The sections below describe the security functionality implemented to ensure the protection of user data.

7.3.1 Access Control

Access control is vital to the prevention of unauthorized use of the system and unauthorized access to and modification of the data in the system. The security functionality described in this section satisfies the SFRs regarding access control; FDP_ACC.1 and FDP_ACF.1.

7.3.1.1 Creation of Privileged Users

Privileged users can only be created at initialization of the TOE and later by other privileged users who have been authorized to do so, i.e. the security officers. Roles and privileges are applied to privileged users to enforce what each user is authorized to do, including the creation of new privileged users.

Privileged users are divided by their responsibilities by assigning them one of two roles; Security Officer and User Manager. The initial privileged users created when initializing the TOE are all Security Officers. The Security Officers and no other privileged users are authorized to create other privileged users.

To create a new privileged user, the command used for creating users must be signed by one or more Security Officers to be accepted by the TOE.

For all new privileged users including those created at initialization, the owner is required to be physically present at creation of his user in Signer to ensure the secrecy of his credentials.

7.3.1.2 Creation of Signer Users

Signer users can only be created by privileged users who are authorized to do so by assigned role; the User Manager role. No other privileged users are authorized to create signer users. To create a new signer user, the User manager must be authenticated through the administrator protocol (using the Administration SDK), and it is verified that he is authorized to create signer users. The User Manager initiates the user creation and the authentication data of the new user is created and stored securely.

7.3.1.3 Signer User Maintenance

The maintenance of a signer user is divided into tasks that can be carried out by the owner of the signer user and tasks that can be carried out by privileged users. The owner can only maintain his own R.Signer object and no other signer user can maintain it. Privileged users must be authorized to maintain signer users to be allowed to perform any maintenance tasks. The privileged users who are authorized to perform signer user maintenance are those who have been assigned the role of user manager. Before any maintenance task is carried out, it is verified that the user is authorized to perform the task. This holds for both signer users and user managers.

Generation of a key pair for a user is instigated by a User Manager by assigning the signer user the appropriate privilege to be assigned a key. Before key generation can be commenced it is verified that the privileged user is authorized to generate keys. The generation of the key pair is done by the cryptographic module and then the private key is bound to R.Signer it was created for and who will hereafter be the owner of the key.

The signature verification data consisting of the public key is transformed into a certificate request. The certification is done by a trusted external CA and the resulting certificate is bound to the R.Signer representation.

Multiple cryptographic modules can be used for key generation. This does not pose a problem since the user data, the authorization data, and the binding of data to user is offloaded from the TOE and securely stored externally. Access to the private signing key is only granted to the signer user owning the key. No other signer user or privileged user can access the private signing key.

7.3.1.4 Signing

The DTBS/R is always supplied to the TOE by the Signer as part of the Signature Activation Protocol prior to the signature operation. The DTBS/R can cover multiple documents to be signed and all signing happens under one user session where the user has been properly authenticated.

The TSF verifies the R.SAD as part of the signature activation protocol. The TSF checks that the SAD elements are linked and ensures that the signer user is strongly authenticated. The TOE then establishes the authorization data needed for the signature operation.

The signer user is strongly authenticated and it is verified that the signer user is authorized to create signatures. No one but the owner of the signer user can achieve access to the signing key for creating signatures on behalf of the signer user.

7.3.1.5 TOE Maintenance

The maintenance of the TOE is handled by privileged users with the security officer role. The security officers can manage roles, privileges and configuration of the TOE. Security officers are the only users with privilege to maintain the TOE.

The security officer(s) must be authenticated before maintaining the TOE configuration. The TOE verifies that he is authorized to do maintenance before allowing any maintenance operations. No other users are allowed to use the maintenance functionality.

7.3.2 Information Flow

This section describes security functionality pertaining to flow of information including external storage of user data. This section also describes the security attributes of the signer users and privileged users which are subject to the described data flow. This security functionality satisfies the following SFRs: FDP_IFC.1 and FDP_IFF.1.

The security functionality enforcing confidentiality and integrity during data exchange is also described in this section. The functionality described satisfies FDP_UCT.1 and FDP_UIT.1.

7.3.2.1 Signer Data Exchange

The TOE stores data in an external repository to meet requirements on capacity and redundancy. The signer user data and associated security attributes are always stored together and associated unambiguously to each other. The data is securely exchanged with the external storage.

The information flow is secure as long as the system is properly initialized and signers created properly. The TOE prevents flow of sensitive information when the system has not been initialized.

When the system is initialized and the initial Security Officers are created, these can create other types of privileged users, e.g. User Managers. A User Manager can securely create a representation of a signer user.

The attributes associated with the representation are protected in integrity and when needed also in confidentiality, e.g. the signing key. The TOE supports secure handling of sensitive data included in the signer representation R.Signer.

When a user has been created as described above, the TOE can securely use the Cryptographic Module to generate signer signing key pairs. The TOE can assign R.Signing_Key_Id and R.SVD to the signer representation R.Signer and it protects the R.SVD against modification before it is certified. The signer user can only perform signature and maintenance operations if created and assigned a signing key as described above.

When the TOE receives the R.Signer representation from the external storage the integrity of the data is verified. The unambiguous association between user data and security attributes are upheld for the signer user data and the confidentiality of the data is also secured. The interpretation of the data is as intended, also after external storage.

7.3.2.2 Privileged User Data Exchange

When placing data of privileged users in external storage, it is integrity protected. Privileged user data is always stored with the associated security attributes. The externally stored privileged user data and security attributes are always unambiguously associated to each other.

The information flow is secure as long as the system is initialized and privileged users created according to the documentation. The TOE prevents flow of sensitive privileged user information when the system is not correctly initialized and the privileged user has been authenticated.

When the system is initialized and the initial privileged users are created, it is possible to securely create additional privileged users with the desired roles and privileges. Privileged users of the type Security Officer may then access the security attributes of other privileged users. All privileged users may access their own security attributes.

When the TOE receives privileged user data from external storage, the integrity of the data is verified, before it can be used. The unambiguous association between privileged user data and security attributes are upheld for the privileged user data and the confidentiality of the data is also secured. The interpretation of the data is as intended, also after external storage.

7.3.2.3 Data Transfer Protection

The signer user's private signing key is confidentially stored externally. The private key is never exchanged besides this. A session between signer user and TOE provides a secure channel that allows the signer user to be able to transmit and receive data in a manner protected from unauthorized disclosure. The TOE verifies the integrity of incoming data to protect against any form of modification.

The access control and information flow control are enforced to be able to transmit and receive user data in a manner protected from modification and insertion for all security attributes for R.Signer and R.Priviliged_User and from modification and replay for R.SAD.

It can be determined on receipt of user data whether modification, deletion, and insertion occurred for all security attributes as defined in R.Signer and R.Privileged_User and for R.SAD for modification and insertion. User commands are protected against replay using sequence numbers. As an additional protection against replay of the R.SAD, the user session is bound to specific R.DTBS/R(s). During a given session, only those R.DTBS/R(s) can be signed with the R.SAD. This prevents replay of R.SAD from being used to sign any additional data.

7.4 Identification and Authentication (FIA)

The security functionality described in this section pertains to the identification and authentication of signer users and privileged users in the TOE. First, the signer user security attributes and the binding of these to the signer users and privileged users is described. This covers how the SFRs FIA_ATD.1 and FIA_USB.1 are satisfied. Then authentication is described in detail, covering the security functionality satisfying the SFRs FIA_UAU.1, FIA_UID.2, and FIA_UAU.5.

7.4.1 Security Attributes

Users of the TOE are all associated with relevant security attributes. The TOE maintains security attributes belonging to individual users depending on user type, i.e. whether the user is a signer user or a privileged user. The following security attributes are maintained for each user:

- Signer user: R.Reference_Signer_Authentication_Data, R.Signing_Key_Id, R.SVD, R.Signer, Authentication level
- Privileged user: R.Reference_Priviliged_User_Authentication_Data, Role

When users are created the TOE enforces that the creating privileged user is authorized to create a new user, i.e. he has the role needed for user creation; Security Officer for privileged user creation and User Manager for signer user creation.

Some of the user security attributes (including R.Signing_Key_ID and R.SVD) may initially be empty. R.DTBS/R is not a Signer security attribute, but is supplied by the signer user prior to signature operations.

Users modifying the security attributes of a signer user must be authorized to do so. Owners of a signer user are never allowed to modify any attributes other than those belonging to his own user. Privileged users must be assigned the appropriate privileges to be allowed to maintain the security attributes of a signer user.

7.4.2 Authentication

To perform TOE operations, users must be unambiguously identified and authenticated which associates the user with his and only his security attributes including the privileges determining his authority to interact with the TOE. Identification and authentication mechanisms are separate for privileged users and signer users.

Privileged users must be successfully authenticated before they are allowed to do operations such as creating or managing signer users. The privileged user initiates communication by sending commands signed with a private key which is password protected and placed on his smart card. The password authentication is done outside the TOE. Each command the TOE receives is verified to ensure that it contains a valid signature from the privileged user(s) issuing the command.

The signer user must be successfully identified and authenticated and a session must be created to establish a trusted path before he can perform any security sensitive operations. The TOE employs the use of assertions for authentication of signer users. Identification and authentication of signer users is delegated to external IdP(s).

When the signer user initiates the signing command, the TOE validates the SAD before passing the R.DTBS/R and the R.Authorisation_Data i.e. the private signing key data of the authenticated signer user to the Cryptographic Module for signing. This ensures that identification and authentication of the signer user is done before signing and that the signer user is unambiguously associated with his private signing key.

Since authentication is delegated to external IdP(s), the responsibility of detection of multiple failed logon attempts is then also deferred to the IdP(s). If the validation of an assertion fails, it will be audit logged.

7.5 Security Management (FMT)

The management of the security of the TOE is described in this section and includes the separation of privileged users and their ability to manage the security of the system if authorized to. The SFRs covered in this section are FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, and FMT_SMF.1.

The security protocols of the TOE restricts the creation and management of signer users and privileged users to privileged users who have been assigned the appropriate privileges. The security protocols also restrict the management of system security attributes and data to privileged users of the security officer role. Only secure values are accepted for all security attributes.

Privileged users and signer users are created separately and as different entity types in the system and the type of user is maintained at all times. This implies that any user is either a privileged user or a signer user and thus a signer user never can be a privileged user. Once a user is created as either a signer user or a privileged user, the user type cannot be changed.

The creation and management of signer user security attributes are restricted to privileged users who have been assigned the user manager role. Creation of security attributes, assignment of privileges for being assigned a signing key, generation of R.SVD and R.Signing_Key_Id, and destruction of attributes is only allowed for privileged users who have been authorized to do so. Other management and use of security attributes is restricted to the owner of the R.Signer user. Restricted operations only allowed by the owner includes the ability to query the security attributes and to supply the R.DTBS/R. When signer users are created, restrictive default values are provided for security attributes when relevant.

When the TOE is initialized, two to four initial privileged users with the security officer role are created. Hereafter the ability to create privileged users and to query the security attributes of a privileged user is restricted to privileged users who have been assigned the security officer role. After creation of a privileged user, the security attributes have been assigned to the user. The security attribute representing the role of a privileged user is chosen on user creation and cannot be modified in the user lifetime. The public key for authentication is also assigned at creation.

The ability to modify security data including configuration of privileged user roles is restricted to Security Officers. Through the Administration Client and the Administration SDK, management of signer users, management of privileged users, and configuration management can be performed.

Every command to change the system configuration must be signed by either one Security Officer, or by two Security Officers where dual control is required. When the command arrives at the TOE it is validated against the current privileged user role configuration and it is verified that the signature(s) on the command are valid. If the command is verified and the signing user(s) are authorized to complete the command, the command is handled and the result created. All verification, command handling, and result creation is performed in a single operation inside the TOE to prevent unauthorized access. All system changes are audit logged and thus the state of the TOE can be seen as a series of signed transformations, using audit logged commands, from the initial state to the current state.

7.6 Protection of the TSF (FPT)

The security functionality of the TOE is protected in various ways which will be described in this section. The section describes how the SFRs FPT_RPL.1 and FPT_TDC.1 are satisfied.

The TOE and the cryptographic module reside within the same physical boundary, and are placed within the tamper-protected environment of the HSM. The capability to determine whether tampering has occurred is provided by this environment. If tampering is detected, the Cryptographic Module will cease to function and thus no security operations through the TOE can be performed.

When security functions data is stored outside the TOE, it is integrity protected and the TOE has the capability to consistently interpret security essential data when the data returns to the TOE. Appropriate configuration is essential for protecting the security of the system and only security officers role can configure the TOE.

As described in section 7.3 user data and security attributes are stored securely outside the TOE. The R.SAD is protected from replay by assigning and verifying sequence numbers for user commands. Execution of a command e.g. for initiation of a signature operation is rejected when replay is detected. Replay detection is logged for auditing purposes.

An installation of Signer requires synchronization with an external reliable time source and thus the TOE receives time stamps from the external source.

7.7 Trusted Paths/Channels (FTP)

This section pertains to the means of providing trusted communication between the users and the TSF, and between TSFs and it describes how SFRs FTP_ITC.1 and FTP_TRP.1 are satisfied.

For the privileged user, trusted communication paths are provided between the Administration Client and the TOE and between the Administration SDK and the TOE through the SSA. Each path is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification by means of signed commands. The data communicated over the trusted path is integrity protected and for security relevant data also protected in confidentiality.

Privileged users are permitted to initiate communication via the above mentioned trusted paths. The trusted paths must be used whenever a privileged user uses the Administration Client or Administration SDK for creating other privileged users, creating and maintaining signer users, generating signing key pairs, and performing TOE maintenance. The TOE rejects communication which is not transmitted via the trusted path.

For the Signer User a trusted path is provided between the SIC and the TOE through the SSA relying on signer user authentication for creating an authenticated and confidential channel. The path is logically distinct from other communication paths and provides protection of the communicated data in integrity and confidentiality using the channel and command encryption. The Signer User is through the SIC permitted to initiate communication via the trusted path. The trusted path will be used when generating signer key pairs, maintaining the signer user, and when signature operations are performed.

The TOE and the Cryptographic Module are located within the physical boundary of the same hardware appliance and thus the communicated data is protected from modification and disclosure and no authorization is required.

The TOE will always initiate the communication since the Cryptographic Module does not have any knowledge of the functionality of the TOE. The TOE sends a request and awaits the response for all uses of the Cryptographic Module.

8 Rationale

8.1 Security Requirements Rationale

8.1.1 Security Requirements 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.

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
Security Audit																	
FAU_GEN.1										X							
FAU_GEN.2										X							
Cryptographic Support																	
FCS_CKM.1/RSA			X													X	
FCS_CKM.4			X														
FCS_COP.1			X												X	X	
FCS_RNG.1																	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		X															

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
Maintenance																	
FDP_ACF.1/ Signer Maintenance		X															
FDP_ACC.1/Signer Key Pair Generation			X	X													
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/privilege					X		X										

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
d User																	
~~FDP_ITC.2/Signer~~	~~X~~																
~~FDP_ITC.2/Privileged User~~					~~X~~		~~X~~										
FDP_UCT.1	X																
FDP_UIT.1	X																
Identification and 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									
FMT_MSA.3/Privileged User					X												
FMT_MTD.1								X	X								
FMT_SMF.1									X								
FMT_SMR.2									X								

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
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												
FPT_TDC.1/Audit										X							
Trusted Path/Channels																	
FTP_TRP.1/SSA									X					X			
FTP_TRP.1/SIC												X	X	X			
FTP_ITC.1/CM			X												X		

Table 15

~~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 is described in FIA_ATD.1 and FIA_USB.1.~~

OT.SIGNER_PROTECTION is handled by requirements for management, access control, protection, and exchange of R.Signer in a secure way. (FDP_IFC.1/Signer, FDP_IFF.1/Signer, FDP_UCT.1, FDP_UIT.1 and FPT_TDC.1). The actual description of the data is described in FIA_ATD.1 and FIA_USB.1.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA is handled by FDP_ACC.1/Signer Creation, 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 Cryptographic Module.

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

~~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_ITC.2/Privileged User and FPT_TDC.1).~~ **OT.PRIVILEGED_USER_MANAGEMENT is handled by requirements for access control in FDP_ACC.1/Privileged User Creation and FDP_ACF.1/Privileged User Creation.** The actual description of the data is described in FIA_ATD.1 and FIA_USB.1. Authentication of Privileged Users 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 R.Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/PrivilegUser, FDP_ITC.2/Privileged User and FPT_TDC.1).~~**OT.PRIVILEGED_USER_PROTECTION is handled by requirements for management, access control, protection, and exchange of R.Privileged User in a secure way (FDP_IFC.1/Privileged User, FDP_IFF.1/privileged User, and FPT_TDC.1).** The actual description of the data is described in FIA_ATD.1 and 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 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.

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. **The physical protection is provided by a CM conformant [EN 419 221-5].** 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~~ **from an external source, and the requirement of integrity protection FPT_TDC.1/Audit.**

OT.SAD_VERIFICATION is handled by ~~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 FTP_TRP.1/SSA and FTP_TRP.1/SIC requiring data transmission to be protected in integrity.

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 Cryptographic Module. 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.

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

OT.RANDOM is handled by the cryptographic module (CM). The TOE is implemented as a local application inside the same physical boundaries as the CM and thus fulfills the same requirements for random number generation as the CM as defined in [UT_ST**].**

8.2 SFR Dependencies

The dependencies between SFRs are addressed as shown in

Requirement	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	~~FPT_STM.1~~ **Environment**
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 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_CKM.1
FCS_RNG.1	None	No dependencies
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~~
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

Requirement	Dependencies	Fulfilled by
		FMT_MSA.3/Privileged User
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/Signer~~
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~~
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	
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5/Signer	None	

Requirement	Dependencies	Fulfilled by
FIA_UAU.5/Privileged User	None	
FIA_UID.2	None	
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 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 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_MSA.1/Privileged User FMT_SMR.2
FMT_MSA.3/Signer	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Signer FMT_SMR.2
FMT_MSA.3/Privileged User	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Privileged FMT_SMR.2
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_SMF.1	None	
FMT_SMR.2	FIA_UID.1	FIA_UID.2
FPT_RPL.1	None	
FPT_TDC.1	None	
FTP_TRP.1/SSA	None	
FTP_TRP.1/SIC	None	
FTP_ITC.1/CM	None	

Table 16

8.2.1 Rationales for SARs

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 its use it manage 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.

Bibliography

[eIDAS]	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
[ANSI-X9.62]	ANS X9.62-2005: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) ANSI (American National Standards Institute).
[Assurance]	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
[AGD]	Guidance documentation, AGD_PRE, v. 2.0 and AGD_OPE, v. 3.0.
[Formats]	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.
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5. CCMB-2017-04-001, April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5. CCMB-2017-04-002, April 2017.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5. CCMB-2017-04-003, April 2017.
[ECCBP]	ECC Brainpool Standard Curves and Curve Generation, v1.0, 19.10.2005 / ECC Brainpool, http://www.ecc-brainpool.org/ecc-standard.htm
[EN 419 241-1]	CEN/TS 419 241-1 Security Requirements for Systems Supporting Server Signing. Draft.
[EN 419 241-2]	Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing.
[EN 419 221-5]	CEN/PP 419 221-5 Protection Profiles for TSP Cryptographic modules – Part 5, Cryptographic Modules for Trust Services.
[ETSI EN 319 411-1]	ETSI, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. 2016.
[ETSI TS 119 312]	ETSI, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. 2014.
[ETSI EN 319 401]	ETSI, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, 2016.
[FIPS 186-4]	FIPS PUB 186-4, Digital Signature Standard (DSS) / National Institute of Standards and Technology (NIST), USA, July 2013

[FIPS 197] FIPS PUB 197, Advances Encryption Standard (AES) / National Institute of Standards and Technology (NIST), USA, 26th November 2001

[FIPS 198] FIPS PUB 198, The Keyed-Hash Message Authentication Code (HMAC) / National Institute of Standard and Technology (NIST), USA, 6 th March 2002

[NIST SP 800-38A] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: Methods and Techniques / National Institute of Standards and Technology (NIST), USA, December 2001.

[NIST SP 800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007.

[NIST SP 800-108] NIST Special Publication 800-108: Recommendation for Key Derivation Using Pseudorandom Functions (Revised) / National Institute of Standards and Technology (NIST), USA; October 2009.

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard.

[RFC2104] RFC 2104: HMAC: Keyed-Hashing for Message Authentication, Internet Engineering Task Force (IETF), February 1997

[SOGIS] SOG-IS, SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, version 1.0, 2016.

[ISO/IEC 19790] ISO/IEC 19790:2012 Information technology – Security techniques – security requirements for cryptographic modules.

[UT_ST] CryptoServer. Security Target Lite for CryptoServer Se-Series Gen2 CP5, version 1.0.0, August 2018. Certification ID: NSCIB-CC-16-119032.