ETUGRA SAM v1.4 Security Target

Document Title: eTugra SAM Security Target

Document Version: 10

TOE Reference: eTugra SAM

Product Type: QSCD

Date: January 09, 2024

Table of Contents

1 Introduction

This Security Target (ST) document defines the security objectives and requirements, as well as the scope of the Common Criteria evaluation of eTugra SAM product. The TOE of this ST i.e., eTugra SAM is loaded as application in the Application Server and interacts with EN 419 221-5 [7] HSM. TOE is a software component loaded into a tamper protected hardware device to ensure a secure execution environment.

This section provides document management and information required for a security target. Section 1.1 “ST Reference” explains the descriptive information necessary for registering the security target. The section 1.2 “TOE Reference” explains the identification information of the TOE. Section 1.3 “TOE Overview” summarize the TOE in narrative form and section 1.4 “TOE Description” contains information about the TOE including the major security features and operational environment.

1.1 ST Reference

This ST is identified by the following unique reference: -

Table 1-1 ST Reference

ST Title:	eTugra SAM Security Target
ST Version	V10
ST Date:	**Error! Reference source not found.**09
ST Author:	E-TUGRA EBG BİLİŞİM TEKNOLOJİLERİ VE HİZMETLERİ ANONİM ŞİRKETİ

1.2 TOE Reference

The TOE is identified by the following unique reference: -

Table 1-2 TOE Reference

TOE Name	eTugra SAM v1.4
TOE short name	eTugra SAM
TOE Version	V1.4
Evaluation Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
Protection Profile(s)	EN 419 241-2 [5]
Evaluation Assurance Level	EAL 4 augmented by AVA_VAN.5
Developer	E-TUGRA EBG BİLİŞİM TEKNOLOJİLERİ VE HİZMETLERİ ANONİM ŞİRKETİ
Evaluation Sponsor	E-TUGRA EBG BİLİŞİM TEKNOLOJİLERİ VE HİZMETLERİ ANONİM ŞİRKETİ
Evaluation Facility	CCLab Software Laboratory
Certification Body	OCSI

TOE version has the version number scheme to identify the current and future versions of the TOE. Current version in the scope of TOE is v1.4.

1.3 TOE Overview

TOE is eTugra Signature Activation Module (SAM) solution. eTugra SAM is deployed by Trust Service Providers (TSPs) as Trustworthy System Supporting Server Signing (TW4S) which supports both remote signatures & sealing (as defined in EN 419 241-1 [6]). The main goal of eTugra SAM is to ensure that the Signer's signing key or keys are only used under the sole control of the Signer and only used for the intended purpose by both users for remote signatures and sealing.

The system uses an EN 419 221-5 [7] Thales Luna K7 Cryptographic module (CM) to generate signing/sealing keys and generate signature values using those keys. CM is an HSM which provides the cryptographic functionality. TOE is able to authenticate signer users and establish relationship between users and keys. These keys are protected keys and no other signer users can get access over other signer users key to apply signature operations. Details related to Thales Luna K7 can be found here[27] and here[28].

TOE defines two types of privileged users (User Managers and Authenticated Applications i.e., Server Signing Applications). TOE authenticates both User Managers and Authenticated Applications before executing any operations. Privileged users are divided by their role to indicate which tasks they can perform:

- **User Managers:** Manages the TOE, create new roles / operators and performs TOE configurations
- **Authenticated Applications (SSA):** Management of signer user keys, sealing keys and invoke cryptographic functions

Signer users are not managed by the TOE directly, instead it is managed by the authenticated applications SSA and is stored in the SSA DB.

Signature Creation Application (SCA) acting as business application interacts with SSA to sign document / transaction and provides the hash to be signed. Signer user authentication is performed indirectly by TOE either through IdP or a mobile application via SSA. Signer user authentication assertion, DTBS/R along with signer key identifier is attached in the Signature Activation Data (SAD). SAD is shared with TOE over Signature Activation Protocol (SAP). TOE verifies the SAD and assertion before signer user key is activated to produced qualified signature.

1.3.1 TOE Type

TOE is a software component loaded into tamper protected hardware device to ensure a secure execution environment. The TOE and the CM are together the Qualified Signature Creation Device (QSCD) named as eTugra SAM QSCD. The TOE provides a remote Qualified Electronic Signatures and Seals (referred to collectively as QES) service according to eIDAS Regulation No 910/2014 [8] at Sole Control Assurance Level 2 (SCAL2) according to EN 419 241-1 [6].

This ST addresses the following advanced security mechanisms: -

- Remote QES according to eIDAS Regulation No 910/2014 [8]; and
- Sole Control Assurance Level 2 (SCAL2) according to sec. 5.4 of EN 419 241-1 [6].

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

1.3.2 TOE Usage & Major Security Features

The major usage and security features of the TOE are:

1. **TOE Setup**
    a. TOE provides interfaces for the TOE setup and creation of privileged users
2. **Operator management**
    a. User Managers create more roles and User Managers which can define other operators / security officers which can approve configurations
    b. User Managers create authenticated applications
3. **Signer User management**

a. Signer user is authenticated indirectly by the TOE. An external IdP or a mobile application via SSA authenticates the Signer user and issues an assertion. SSA passes this assertion in the SAD to SAM.

b. Authenticated applications generate signing / sealing keys and Signature Verification Data (SVD) using a CM and bind signing key ID and SVD to a signer user

c. Authenticated applications can disable a signing key identifier to be used by a signer

4. **Signature operation**

   a. Signer users interacts with business application (SCA) to sign a document

   b. Business application (SCA) interacts with authenticated applications (SSA) and provides hash to be signed

   c. Signer authentication along with DTBS/R, signing key identifier is bound together within the Signature Activation Data (SAD). SAD is securely exchanged with the TOE over the Signature Activation Protocol (SAP). TOE performs the following operations on the SAD before the signature operation is performed on the DTBS/R

      i. TOE verifies the SAD integrity

      ii. Signer user identity is authenticated via provided SAD. TOE follows the indirect authentication of the signer user as signer user is authenticated by external IdP or a mobile application via SSA which produces an assertion. This assertion is part of the SAD.

      iii. DTBS/R is taken from the provided SAD before signature operation performed

      iv. Signing Key identifier is taken from the SAD and linked with the signer user

      v. TOE receives the authorisation data to activate the signing key referred to by the Signing Key Identifier from the SSA, and then interacts with Cryptographic module (CM) to perform signature operations

5. **Audit logs**

   TOE generates complete audit logs for each operation performed in the TOE either by User Managers, authenticated applications, interaction with CM Audit log integrity is also ensured. System administrators can access the audit logs and its outside the scope of TOE. Audit logs are accessible via system operations and are stored in a file which is being rotated based on the configurations

defined. To protect the integrity of the contents in the log file, digital signature is applied on the log file. The path for the storage of log file is also configurable and defined by System administrator and access to that storage area is restricted to authorised representatives only. System administrators can apply the log file configuration and this is outside of TOE scope.

eTugra SAM QSCD can be deployed in high availability with load balancer in front of it to manage the traffic. Cryptographic keys replication from one eTugra SAM QSCD to the other is supported through the CM utilities.

1.3.3 TOE Life Cycle

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

1. **Development:** The TOE developer develops the TOE application and its guidance documentation using any appropriate guidance documentation for components working within the TOE physical boundary, including the CM.
2. **Delivery:** The TOE is securely delivered from the TOE developer to the TSP. TOE is delivered to TSP through secure authenticated mutual channel and SHA256 checksum is also provided. TOE package is embedded into eTugra SAM QSCD. TSP verifies the SHA256 checksum before utilization.
3. **Installation and configuration:** The TSP install and configure the TOE with the appropriate configuration and initialisation data.
4. **Operational phase:** In operation, the TOE can be used by privileged users i.e. User manager Operators to create other Privileged Users (User Managers and Authenticated Applications (SSAs)). User Managers can maintain TOE configuration. Authenticated applications can manage Signers accounts and generate signature keys for a Signer. Authenticated applications supply the data to be signed to the TOE and only Signers can authorise a signature creation

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

1.3.4 TOE Environment

TOE and CM certified against EN 419 221-5 [7] is required to obtain a QSCD i.e. eTugra SAM QSCD. TOE is software component deployed in secure tamper protected environment which interacts with CM i.e. HSM to perform key generation and signature operations. Once the TOE is setup, signer user in local environment interacts with authenticated application i.e. Server Signing Application (SSA) which is

registered in TOE as privileged user. SSA holds the complete signer user information which includes signing key identifier. To perform the signature operation the SAP is used, the SAD is provided using the SAP along with other information. SAD binds the signer user authentication factor, signing key identifier, validity and DTBS/R.

Before signature operation is performed, TOE job is to ensure that signer user has sole control of his signing / sealing keys. TOE ensures that it validates the SAD integrity, verify SAD, verifies the bindings of SAD elements and then finally activate the signing key in CM to perform signature operation. During the SAD elements binding validation, TOE ensures that signer user is authenticated well before signature operation is triggered in the CM. TOE and CM are located in secure tamper protected environment.

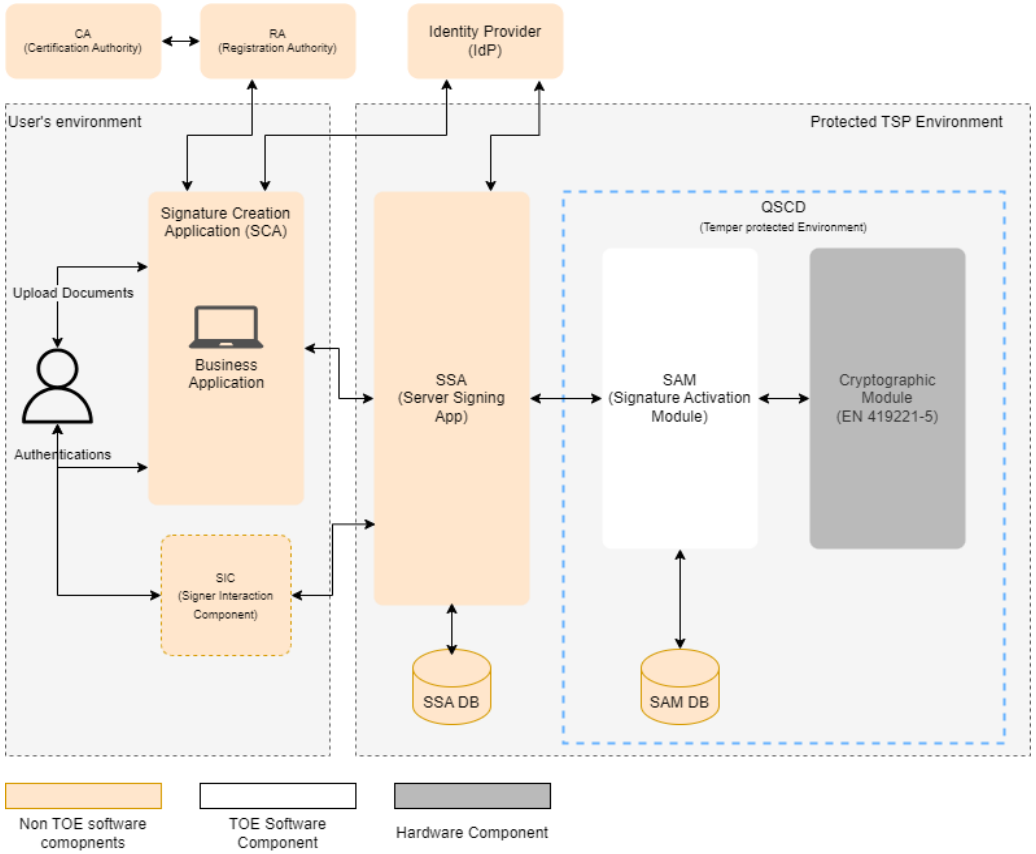

Fig 1. Architecture of TOE

Signer user authentication is not performed by the TOE directly, instead it is delegated to other component or external Identity Provider (IdP) which meets the EN 419 241-1 [6] requirements required for qualified signatures. IdP holds multiple authentication factors for the

signer users defined in EN 419 241-1 [6]. Once signer user is authenticated IdP or other component provides the assertion or token and it is verified by the TOE.

Before signature operation is performed by CM via TOE, signer user interacts with SSA via standard interfaces. The signer user uses Signature Interactive Component (SIC) based as defined in EN 419 241-1 [6] to communicate securely with SSA. SSA then forwards the received communication from signer user via SIC to eTugra SAM QSCD. The QSCD holds the TOE and CM, TOE handles the traffic from SSA and verifies the provided SAD and invokes CM over secure authenticated channel to trigger signature operation using the supplied key identifier and then returns the signature value back to SSA which then provides it to business application (SCA) with which signer user was interacting for signing the document. The signing or sealing key is generated earlier in the CM before signature operation is started. These keys are requested by the SSA via authenticated application APIs on behalf of signer user. TOE generates complete audit logs for each operation performed by the privileged users. In this case it would be SSA acting as authenticated application. This way, all the activities of SSA are auditable.

TOE is setup via administrative interfaces which might require approval of another operator before any configuration is pushed into TOE database.

TOE doesn't interact with any other application except SSAs. In order to perform operations SSA must be initialized, connected securely with TOE and configured as trusted authenticated application in the TOE. Industry standard secure protocols are implemented in SSA which business application or signing creation application (SCA) can implement to interact with SSA for signer user on-boarding and signing. SIC is installed on signer user premises which interacts with SSA for the signature operation. SIC to SSA communication is performed on secure channel.

1.3.5 Non-TOE Hardware/Software/Firmware

TOE requires the following components to perform its operations:

1. Cryptographic module (CM) certified against EN 419 221-5 [7] which generates signer user signing / sealing keys and activate key to perform signature operations
2. RDBMS Server (SAM DB) which holds the information and a file-based storage system to hold the generated audit logs
3. Business application or signature creation application (SCA) that holds the document to be signed and sends the hash to SSA

4. Server Signing Application (SSA) which holds the signer user information and provides interfaces for signer user on-boarding, SIC interface and then interacts with SAM located inside QSCD
5. Signature Interactive Component (SIC) held by signer user in its local environment which interacts with SSA using standard secure protocols to perform SIC operations
6. Reliable time source
7. An external Identity Provider (IdP) which meets the EN 419 241-1 [6] requirements and holds the authentication factors for the signer user. The IdP authenticates the user and provides an authentication assertion or token to the TOE for verification.
8. eTugra SAM QSCD is authenticated from Active Directory and receives an encrypted Kerberos ticket. This Kerberos ticket is being exchanged during secure channel with Fortigate which provides reliable time source. Fortigate is general element in the operational environment which holds the features of integration with Active Directory. Fortigate / FortiOS 7.0.7 is CC Certified but currently the latest version is being used.

1.4 TOE Description

eTugra SAM which fulfills the EN 419 241-2 requirements and hosted in tamper protected environment. It interacts with CM (Signature Creation Device (SCDev) as defined in 419 241-1 [6]) for the signer user signing /sealing key generation and signing. SAM verifies the SAD produced as a result of authorization by the signer through SIC to activate the signer key to perform signing operation. SAM delegates the signer authentication to external identity provider (IdP). SAM uses database to store the TOE configurations and privilege user information.

eTugra SAM is designed to contain two types of interfaces to perform the TOE desired operations:

- Administrative Interface
- Service Interface

1.4.1 Physical Scope of the TOE

The TOE is software component loaded into the tamper protected hardware fulfilling requirements of ISO/IEC 19790 [22] Security Level 3. More details of tamper protected hardware can be found in the AGD guidance documents [25] & [26]. The tamper protected hardware is also part of the TOE but not everything inside is part of the TOE. The operating system, application server, CM, database do not belong to the TOE.

TOE is retrieved through an authenticated channel and loaded into tamper protected hardware. It includes SAM package, HSM client and documentation. SAM software package is a zip file which includes all the executables e.g., binaries and related configuration files. Similarly, HSM client is a zip file which includes all of the dependencies required for the HSM client installation. The SAM guidance documentation files are labelled with PDF extension.

- e-Tugra SAM Installation Guide.pdf (v5)
- eTugra-SAM-User-Guide.pdf (v2)
- AGD_OPE – Operational User Guidance (v9)
- AGD_PRE – Preparative procedures (v8)

1.4.2 Logical Scope of the TOE

When TOE is deployed in tamper protected environment, it allows to perform remote signatures and seals. There are several logical entities involved which covers TOE setup, administration.

1.4.2.1 TOE setup

When TOE is deployed, it can’t be used unless it’s initialized and configured properly. An authenticated User Manager Operator must be connected with TOE using Administration interface to setup and initialize the TOE. Another operator with the Security Officer role is used to approve the configuration. The Security Officer must be securely authenticated before configurations of the TOE are pushed.

1.4.2.2 Roles & Available Functions

The TOE maintains the following roles: -

Privileged Users. There are two types of Privileged Users 1) User Managers 2) Authenticated Application i.e. SSA:

a. **User Manager**: It defines different types of roles and operators who can perform configurations and maintenance of TOE. User manager operator can define / configure multiple authenticated application (SSAs) based on the deployment model e.g., Single Instance or HA instances. The User Manager role is further separated into various operators as described in section 3.2.

b. **Authenticated Application (SSA)**: Authenticated application i.e. SSA which interacts with TOE over Service interface to for signer user key generation and signing operations via secure trusted authenticated channel

Unprivileged Users.

a. **Signers**: Those who request for qualified remote signature and seals interact with business applications (SCAs) and utilize SIC component to authorise the signature operation. These business applications (SCAs) use Authenticated Applications (SSA) to create keys or manage signatures.

1.4.2.3 Cryptographic Support

The TOE does not perform cryptographic operations for signers rather it relies on CM. The TOE invokes the CM with appropriate parameters whenever a cryptographic operation for the Signer is required, i.e., to authorise usage of the signing / sealing key.

In addition, TOE invokes CM for additional cryptographic keys which are required for their operations.

1.4.2.4 Audit

TOE generates logs against each operation performed by the TOE. Whenever User manager operator interacts with TOE via Administration interface, log is generated. Similarly, authenticated application i.e., SSA interacts with TOE for signer user signing / sealing keys generation

& signature operations audit data is generated and each information is logged. Audit logs are also generated during SAD verification process. Each audit log entry doesn't contain any sensitive information which can reveal any information about the signer user. Generated audit log entries are protected and integrity is ensured. Audit logs are accessible via system operations and are stored in a file which is being rotated based on the configurations defined. To protect the integrity of the contents in the log file, digital signature is applied on the log file. The path for the storage of log file is also configurable and defined by System administrator and access to that storage area is restricted to authorised representatives only. System administrators can apply the log file configuration and this is outside of TOE scope.

1.4.2.5 Trusted Communication

The TOE enforces the secure trusted communication methods and protocols when privileges users interact with TOE and TOE also establishes a secure channel with CM for cryptographic operations. SIC interaction with SSA is also made over secure authenticated channel. The SAP is protected against replay, bypass and forgery attack, using a salt (random value to avoid replay attack), a validity period and the PKCS#1 authorization signature of the Signer. The SAP provides confidentiality for all sensitive transmitted data and integrity protection for all transmitted data, including the authentication and authorisation data and DTBS/R.

1.4.2.6 Signer User Keys Generation

Signers are not managed by the TOE therefore no information about signers is stored by the TOE. Instead, this information is stored in the SSA. When signer user is created in SSA, no key is associated with it. The key generation request is sent to SSA by the business application which relays the request to TOE. TOE triggers key generation in CM and encrypted signer keys ,key handles andpassphrase are sent back to SSA for storage. Signing keys details are stored securely by the SSA and integrity ensured for them along with signer user information. Business application controls the creation of signer users via requesting the SSA application. SSA stores the information related to the signers. TOE manages signer keys creation using CM.

1.4.2.7 Signing Key Activation

To activate the key in the TOE, signer user must be authenticated via IdP or other component and the assertion should be presented to the SSA. SSA sends the request to TOE via SAD. This ensures that signer holds sole control over his key, which can only be activated after the signer is authenticated and can't be used by any other signer.

1.4.2.8 SAP and signature

Signer holds the Signature Interactive Component (SIC) which interacts with SSA over Signature Activation Protocol (SAP) using a secure trusted channel. If signer authentication is successful and assertions are verified then TOE activates the signer key and signature operation is performed by CM referencing the right Key Identifier.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This ST claims conformance to: -

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 [1].
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017,[3].

as follows: -

Part 2 extended; and

Part 3 conformant.

The following must be considered: -

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4].

2.2 Package Conformance Claim

This ST claims conformance to: -

- EAL 4 assurance package augmented by AVA_VAN.5 defined in the CC Part 3 [3].

2.3 Protection Profile Conformance Claim

This ST claims strict conformance to: -

- EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing [5].

2.4 Protection Profile Conformance Rationale

2.4.1 Security Problem Definition

This ST claims strict conformance to the EN 419241-2:2019 [5]. The parts of the TOE listed in this standard correspond to the ones listed in section 1.4.1 of this ST.

The security problem definition includes the assets, the subjects, the assumptions, the threats and the organizational security policies of the standard.

The following tables demonstrates that this ST contains all assumptions, threats and organisational security policies listed in EN 419241-2:2019 [5].

Table 2-1 Source of Assumptions

Assumptions	419241-2:2019 [5]	Added by this ST
A.PRIVILEGED_USER	x	
A.SIGNER_ENROLMENT	x	
A.SIGNER_AUTHENTICATION_DATA_PROTECTION	x	

Assumptions	419241-2:2019 [5]	Added by this ST
A.SIGNER_DEVICE	x	
A.CA	x	
A.ACCESS_PROTECTED	x	
A.AUTH_DATA	x	
A.TSP_AUDITED	x	
A.SEC_REQ	x	

Table 2-2 Source of Threats

Threats	419241-2:2019 [5]	Added by this ST
ENROLMENT		
T.ENROLMENT_SIGNER_IMPERSONATION	x	
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED	x	
T.SVD_FORGERY	x	
SIGNER MANAGEMENT		
T.ADMIN_IMPERSONATION	x	
T.MAINTENANCE_AUTHENTICATION_DISCLOSE	x	
USAGE		
T.AUTHENTICATION_SIGNER_IMPERSONATION	x	
T.SIGNER_AUTHENTICATION_DATA_MODIFIED	x	
T.SAP_BYPASS	x	

Threats	419241-2:2019 [5]	Added by this ST
T.SAP_REPLAY	x	
T.SAD_FORGERY	x	
T.SIGNATURE_REQUEST_DISCLOSURE	x	
T.DTBSR_FORGERY	x	
T.SIGNATURE_FORGERY	x	
SYSTEM		
T.PRIVILEGED_USER_INSERTION	x	
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION	x	
T.AUTHORISATION_DATA_UPDATE	x	
T. AUTHORISATION_DATA _DISCLOSE	x	
T.CONTEXT_ALTERATION	x	
T.AUDIT_ALTERATION	x	
T.RANDOM	x	

Table 2-3 Source of Organisational Security Policies

Organisational Security Policies	419241-2:2019 [5]	Added by this ST
OSP.RANDOM	x	
OSP.CRYPTO	x	

2.4.2 Security Objectives

The security objectives of EN 419241-2:2019 [5] are included in this ST.

No additional security objectives were added by this ST.

Table 2-4 Source of Security objectives

	419241-2:2019 PP [5]	Added by this ST
Security Objectives for the TOE		
OT.SIGNER_PROTECTION	x	
OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	x	
OT.SIGNER_KEY_PAIR_GENERATION	x	
OT.SVD	x	
OT.PRIVILEGED_USER_MANAGEMENT	x	
OT.PRIVILEGED_USER_AUTHENTICATION	x	
OT.PRIVILEGED_USER_PROTECTION	x	
OT.SIGNER_MANAGEMENT	x	
OT.SAD_VERIFICATION	x	
OT.SAP	x	
OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	x	
OT.DTBSR_INTEGRITY	x	
OT.SIGNATURE_INTEGRITY	x	
OT.CRYPTO	x	
OT.RANDOM	x	

	419241-2:2019 PP [5]	Added by this ST
OT.SYSTEM_PROTECTION	x	
OT.AUDIT_PROTECTION	x	
Security Objectives for the operational environment		
OE.SVD_AUTHENTICITY	x	
OE.CA_REQUEST_CERTIFICATE	x	
OE.CERTIFICATE_VERFICATION	x	
OE.SIGNER_AUTHENTICATION_DATA	x	
OE.DELEGATED_AUTHENTICATION	x	
OE.DEVICE	x	
OE.ENV	x	
OE.CRYPTOMODULE_CERTIFIED	x	
OE.TW4S_CONFORMANT	x	

2.4.3 Security Functional Requirements

The functional requirements described in section 6 of this ST include all SFRs from EN 419241-2:2019 [5].

Iterations and changes to the SFRs, with respect to EN 419241-2:2019 [5], are listed in this table. These changes do not lower TOE security.

Table 2-5 Source of Security functional requirements

Security Functional Requirement	419241-2:2019 PP [5]	Changes by this ST
Security Audit		
FAU_GEN.1.	x	

Security Functional Requirement	419241-2:2019 PP [5]	Changes by this ST
FAU_GEN.2	x	
Cryptographic Support		
FCS_CKM.1	x	iterated to */RSA, */ECDSA, */AES
FCS_CKM.4	x	
FCS_COP.1	x	iterated to */DIG_SIG_GEN, */DIG_SIG_VER, */HASH, */HMAC, */ENC
FCS_RNG.1	x	
User Data Protection		
FDP_ACC.1/Privileged User Creation	x	added refinement
FDP_ACF.1/Privileged User Creation	x	added refinement
FDP_ACC.1/Signer Creation	x	added refinement
FDP_ACF.1/ Signer Creation	x	added refinement
FDP_ACC.1/Signer Key Pair Generation	x	added refinement
FDP_ACF.1/Signer Key Pair Generation	x	added refinement
FDP_ACC.1/Signer Maintenance	x	added refinement
FDP_ACF.1/Signer Maintenance	x	added refinement
FDP_ACC.1/Signer Key Pair Deletion	x	added refinement
FDP_ACF.1/Signer Key Pair Deletion	x	added refinement

Security Functional Requirement	419241-2:2019 PP [5]	Changes by this ST
FDP_ACC.1/Supply DTBS/R	x	added refinement
FDP_ACF.1/Supply DTBS/R	x	added refinement
FDP_ACC.1/Signing	x	
FDP_ACF.1/Signing	x	
FDP_ACC.1/TOE Maintenance	x	added refinement
FDP_ACF.1/TOE Maintenance	x	added refinement
FDP_ETC.2/Signer	x	
FDP_IFC.1/Signer	x	added refinement
FDP_IFF.1/Signer	x	added refinement
FDP_ETC.2/Privileged User	x	
FDP_IFC.1/Privileged User	x	added refinement
FDP_IFF.1/Privileged User	x	added refinement
FDP_ITC.2/Signer	x	
FDP_ITC.2/Privileged User	x	
FDP_UCT.1	x	
FDP_UIT.1	x	
Identification and Authentication		
FIA_AFL.1	x	iterated to */SSA, */User Manager
FIA_ATD.1	x	

Security Functional Requirement	419241-2:2019 PP [5]	Changes by this ST
FIA_UAU.2	x	
FIA_UAU.5/Signer	x	
FIA_UAU.5/Privileged User	x	added refinement
FIA_UID.2	x	
FIA_USB.1	x	added refinement
Security Management		
FMT_MSA.1/Signer	x	added refinement
FMT_MSA.1/Privileged User	x	added refinement
FMT_MSA.2	x	
FMT_MSA.3/Signer	x	added refinement
FMT_MSA.3/Privileged User	x	added refinement
FMT_MTD.1	x	added refinement
FMT_SMF.1	x	
FMT_SMR.2	x	added refinement
Protection of the TSF		
FPT_PHP.1	x	
FPT_PHP.3	x	
FPT_RPL.1	x	
FPT_STM.1	x	
FPT_TDC.1	x	
Trusted Path/Channels		

Security Functional Requirement	419241-2:2019 PP [5]	Changes by this ST
FTP_TRP.1/SSA	x	added refinement
FTP_TRP.1/SIC	x	
FTP_ITC.1/CM	x	

2.4.4 Security Assurance Requirements

The minimum package of security assurance requirement allowed for conformance to EN 419241-2:2019 PP [5] is EAL 4 augmented with AVA_VAN.5.

This ST claims conformance to EAL 4 augmented by AVA_VAN.5. Therefore, the afore-described requirement is met and with respect to EN 419241-2:2019 PP [5].

3 Security Problem Definition

3.1 Assets

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

Application Note 1 (Application Note 1 from [5])

The integrity and confidentiality of the signing key and the link between the R.Signing_Key_Id and the signing key is the responsibility of the CM. 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 CM. The signing key is identified by R.Signing_Key_Id. It shall be protected in integrity and confidentiality.

Application Note 2 (Application Note 2 from [5] , refined by the ST Author)

The R.Authorisation_Data is used by the CM to activate a signing key. During signing key pair generation, the TOE generates a reference passphrase, and returns it to the SSA. During signing the TOE receives passphrase linked against each signer key from the SSA which acts as the R.Authorisation_Data. To ensure the confidentiality, passphrase is stored in encrypted form in SSA and transmitted to TOE over secure channel. The TOE shall verify the SAD before the R.Authorisation_Data is used to activate the signing / sealing key in the CM.

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

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

R.DTBS/R: set of data which is transmitted to the TOE for digital signature creation on behalf of the signer. The DTBS/R is transmitted to the TOE. The R.DTBS/R shall be protected in integrity. 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 (Application Note 3 from [5])

The confidentiality of the R.DTBS/R is not required by eIDAS Regulation No 910/2014 [8].

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

- The signer's strong authentication as specified in EN 419 241-1 [6].
- 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 (Application Note 5 from [5])

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 (Application Note 6 from [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.

R.Signing_Key_Id is <CertificateID> of the certificate assigned to the R.Signer.

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

R.Audit: is an audit record that contains a log of events, which require audit. The logs are produced by the TOE and stored externally. The R.Audit shall be protected in integrity.

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

Each audit entry recorded is protected in its 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 7 (Application Note 7 from [5])

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 8 (Application Note 8 from [5])

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

Application Note 9 (Application Note 9 from [5], refined by ST Author)

The TOE does not persistently store the R.Signer object. The Signer account information is stored by the SSA instead.

R.Reference_Signer_Authentication_Data: is the set of data used by TOE to authenticate the signer. The Signer is authenticated by the IdP, which provides an assertion to the TOE. The SSA is the authenticated application that connects with the SAM to provide the SAD, which contains the assertion of Signer authentication from the IdP. The SSA computes the SAD which contains the received assertion either from

IdP or other component[1] along with assertion certificate which can be used by TOE to verify the integrity of the received assertion and extracts signer information from the received assertion.

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

Application Note 10 (Application Note 10 from [5])

The R.Reference_Signer_Authentication_Data are used by the TOE to authenticate the signer, and the R.Authorisation_Data are 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 11 (Application Note 12 and 13 from [5])

The TOE configuration data includes but not limited to: -

[1] Note that references to the IdP assertion throughout this ST equally apply to an assertion provided by the SIC

- CM configuration;
- Creation of User manager operators;
- Creation of authenticated application

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**: 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 their signing key in the CM. They are able to perform signing operations (authorising their signing keys in the CM, transmitting the required data, including the unique user ID, two different authentication factors, the key ID, the key Authorisation Data and DTBS/R(s))
- **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. There are two types of Privileged Users: **User Managers** and **Authenticated Applications (SSAs)**.
    - User Managers are able to create additional privileged user within the TOE. There are different types of roles for User Manager:
        - Administrator: responsible for maintaining and configuring the TOE
        - Security Officer: responsible for approving TOE configurations

- Authenticated Applications (SSAs) are responsible for Signer key management and invoking cryptographic functions (Signer user creation, signing key generation, signing)

Application Note 12 (Application Note 16 from [5])

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 [11]

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: -

- Transferring wrong R.Signer to TOE from RA; or
- Transferring wrong R.Reference_Signer_Authentication_Data to TOE from RA.

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

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

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

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

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

The asset R.Reference_Signer_Authentication_Data is threatened.

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

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

T.SVD_FORGERY

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

The asset R.SVD is threatened.

If the CA relies on the generation of the key pair controlled by the TOE as specified in ETSI EN 319 411-1 [11] clause 6.3.3 d) then an attacker can forge signatures masquerading as the signer.

Application Note 13 (Application Note 17 from [5], refined by ST author)

There must be secure transport of R.SVD from TOE to RA or CA systems. SAM only generates the 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 the Signer.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

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

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

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

3.3.3 Usage

This section describes threats for signature operation including authentication.

T.AUTHENTICATION_SIGNER_IMPERSONATION

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

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_Authentication_Data is threatened.

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

T.SAP_BYPASS

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

The asset R.SAD is threatened.

T.SAP_REPLAY

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

The asset R.SAD is threatened.

T.SAD_FORGERY

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

The asset R.SAD is threatened.

T.SIGNATURE_REQUEST_DISCLOSURE

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

The 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 R.DTBS/R.

The assets R.DTBS/R and R.SAD are 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 14 (Application Note 18 from [5])

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 15 (Application Note 19 from [5], refined by ST author)

It is not sufficient for an attacker to access R.Authorisation_Data and R.Signing_Key_Id to activate the signing key within CM (the SAM URL and valid authenticated application credentials are also required). Both R.Signing_Key_Id and passphrase (R.Authorisation_Data) are protected in integrity. Access to R.Authorisation_Data is allowed to authorised authenticated operators in TOE.

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 unauthorised operation.

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

T.AUDIT_ALTERATION

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

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

T.RANDOM

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

The asset R.Random is threatened.

3.4 Relation Between Threats & Assets

This following table provides an overview of the relationships between asset, associated security properties and threats. For details consult the individual threats in the previous sections. (The table does not contain information where the confidentiality requirement is considered fulfilled)

Table 3-1 Overview of the relationship between asset, associated security properties and threats

Asset	Security Dimensions	Threats
R.Signing_Key_Id	Integrity	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUTHORISATION_DATA_UPDATE T.AUTHORISATION_DATA_DISCLOSE
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_DISCLOSURE T.DTBSR_FORGERY T.AUDIT_ALTERATION
	Origin authentication	T.DTBSR_FORGERY

Asset	Security Dimensions	Threats
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.SIGNATURE_REQUEST_DISCLOSURE T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrity	T.SIGNATURE_FORGERY T.AUDIT_ALTERATION
R.Audit	Integrity	T.AUDIT_ALTERATION
R.Signer	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION T.AUDIT_ALTERATION

Asset	Security Dimensions	Threats
R.Reference_Signer_Authentication_Data	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTHENTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Confidentiality	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTHENTICATION_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

Asset	Security Dimensions	Threats
R.RANDOM	Integrity	T.RANDOM
	Confidentiality	T.RANDOM
R.TSF_DATA	Integrity	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

3.5 Organisational Security Policies

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

OSP.RANDOM

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

OSP.CRYPTO

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

Application Note 16 (Application Note 20 from [5])

For cryptographic algorithms within the European Union this is as indicated in eIDAS [8] and an exemplary list of algorithms and parameters is given in ETSI TS 119 312 [9] or SOG-IS [10].

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 [8]. Guidance for how to implement an enrolment and certificate management system in conformance with [8] are given in e.g. EN 319 411-1 [11] or for qualified certificate in e.g. EN 319 411-2 [12].

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

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

A.SIGNER_DEVICE

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

A.CA

It is assumed that the qualified TSP that issues Signer qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in eIDAS [8].

A.ACCESS_PROTECTED

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

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

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

Application Note 17 (Application Note 21 from [5])

All the data (Signer information and key details that are stored in the SSA) are stored outside the TOE protected in the 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 shall be assumed that the SAD was submitted under the full control of the Signer by means that are in possession of the Signer.

A.TSP_AUDITED

It is assumed that the TSP deploying the SSA and TOE is a qualified TSP according to article 3 (20) of eIDAS Regulation (EU) No 910/2014 [8] and audited to be compliant with the requirements for TSP's given by eIDAS [8].

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[6].

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 is protected in integrity and if needed in confidentiality.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

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

OT.SIGNER_KEY_PAIR_GENERATION

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

OT.SVD

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

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 18 (Application Note 22 from [5])

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 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 19 (Application Note 24 from [5])

Requirements for authentication are described in EN 419 241-1 [6] SRA_SAP.1.1.

OT.SAP

The TOE shall implement the server-side endpoint of an 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; and
- Protection against replay, bypass of one or more steps and forgery.

Application Note 20 (Application Note 25 from [5])

The Signer authentication is assumed to be conducted according to EN 419 241-1 [6] SCAL.2 for qualified signatures. This means Signer authentication can be carried out in the following way: -

- 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.

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 authorised by Privileged User and that unauthorised modification can be detected.

OT.AUDIT_PROTECTION

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

4.2 Security Objectives for the Operational Environment

OE.SVD_AUTHENTICITY

The operational environment shall ensure the SVD integrity during transmission 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 [8].

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

Since the TOE has support for and is configured to use delegated authentication, the TSP deploying the SSA and TOE shall ensure that all requirements in EN 419 241-1 [6] 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 eIDAS Regulation (EU) No 910/2014 [8]; 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 eIDAS Regulation (EU) No 910/2014 [8].

If the Signer is only authenticated using a delegated party, the TSP shall ensure that the secret key material used to authenticate the delegated party to the TOE shall reside in a certified CM consistent with the requirement as defined in EN 419 241-1 [6] SRG_KM.1.1.

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 [6]. 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 eIDAS Regulation (EU) No 910/2014 [8] and audited to be compliant with the requirements for TSP's given by eIDAS [8]. The audit of the qualified TSP shall cover the security objectives for the operational environment specified in this clause.

The TOE shall operate in a protected environment that limits physical access to the TOE to authorised privileged users. The TOE software and hardware environment (including client applications) shall be installed and maintained by Privileged Users 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

The TOE is implemented as a local application within the same tamper protected physical boundary as the CM defined in EN 419 221-5 [7], but is not contained within the CM. The TOE relies on the CM 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 [7]

Application Note 21 (Application Note 26 from [5], refined by ST author)

The ST is comformant to the PP (EN 419 241-2 [5]), and is is implemented as separate application and both TOE and CM are residing in the same physical boundary in tamper protected environment

OE.TW4S_CONFORMANT

The TOE shall be operated by a qualified TSP in an operating environment conformant with EN 419241-1 [6].

4.3 Security Problem Definition & Security Objectives

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

Table 4-1 TOE Security objectives (Enrolment) 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.SIGNATURE_REQUEST_DISCLOSURE					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
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					
T.RANDOM					

Table 4-2 TOE Security objectives (Signer Management and System) and threats

	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.SIGNATURE_REQUEST_DISCLOSURE									
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 4-3 TOE Security objectives (Usage) and threats

	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							
T.RANDOM							

Table 4-4 TOE Security Objectives and Organizational Security Policies

	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 4-5 Threats and Security Objectives for the environment

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DELEGATED_AUTHENTICATION	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.SIGNATURE_REQUEST_DISCLOSURE								
T.DTBSR_FORGERY					X			
T.SIGNATURE_FORGERY								
System								
T.PRIVILEGED_USER_INSERTION								
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION								
T.AUTHORISATION_DATA_UPDATE								
T.AUTHORISATION_DATA_DISCLOSE								
T.CONTEXT_ALTERATION								
T.AUDIT_ALTERATION								
T.RANDOM								

[2] The TOE uses delegated authentication.

Table 4-5 Organizational Security Policies and Security Objectives for the environment and Assumptions and Security Objectives for the environment

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

A.SEC_REQ									X

4.4 Rationale for the Security Objectives

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

4.4.1 Threats & Objectives

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

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

It is also covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring the TOE to be able to assign Signer authentication data to the R.Signer.
It is also covered by OE.TW4S_CONFORMANT as that requires signer enrolment to be handled in accordance with [14] 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 CM to generate signer key pair.
It is also covered by OT.SVD requiring the SVD to be protected while inside the TOE.

It is also covered by OT.CRYPTO requiring the usage of endorsed algorithms.
It is also covered by OE.SVD_AUTHENTICITY requiring the environment to protect the SVD during transmit from the TOE to the CA.
It is also covered by OE.CA_REQUEST_CERTIFICATE requiring the certification request to be protected in integrity.

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

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

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

T.SAP_REPLAY is covered by OT.SAP requiring that the SAP shall be able to resist whole or part of it being replayed.
It is also covered by OE.DEVICE requiring the SIC to participate the in SAP.

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

T.DTBSR_FORGERY is covered by OT.DTBSR_INTEGRITY requiring the R.DTBS/R to be protected in integrity during transmit to the TOE.
It is also covered by OE.DEVICE requiring the SIC to participate in the SAP.

T.SIGNATURE_FORGERY is covered by OT.SIGNATURE_INTEGRITY requiring that the signature is protected in integrity inside the TOE.
It is also covered by OT.CRYPTO requiring the usage of endorsed algorithms.

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

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION is covered by OT.PRIVILEGED_USER_MANAGEMENT requiring only Privileged User can modify R.Privileged_User and OT.PRIVILEGED_USER_AUTHENTICATION that requires a Privileged User to be authenticated.
It is also covered by OT.PRIVILEGED_USER_PROTECTION requiring the Privileged User to be protected in integrity.

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

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

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

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

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

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 their 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.

4.4.2 Organizational Security Policies & Objectives

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

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

4.4.3 Assumptions & Objectives

A.PRIVILEGED_USER is covered by OE.TW4S_CONFORMANT which requires that the system where the TOE operates is compliant with EN 419 241-1 [6] where clause SRG M1.8 requires that administrators are trained.

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

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

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

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

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

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

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

A.SEC_REQ is covered by OE.TW4S_CONFORMANT requiring the system where the TOE operates is compliant with EN 419 241-1 [6].

5 Extended Components Definitions

5.1 Class FCS: Cryptographic Support

The Class FCS: Cryptographic Support as defined in CCPART2 [2] 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:

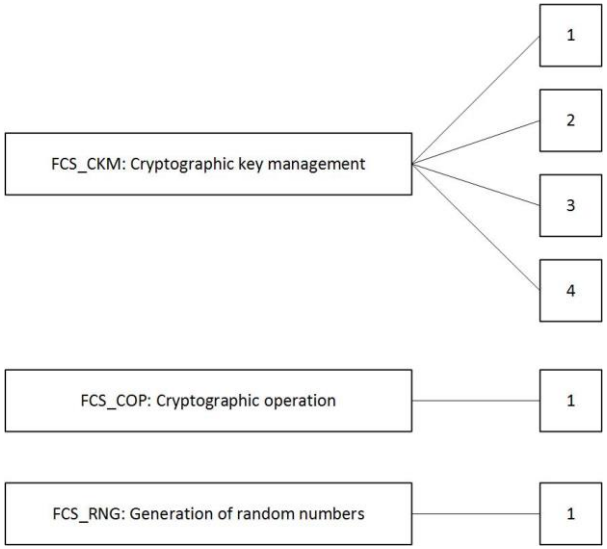

Fig 2. Cryptographic Support

5.2 Generation of Random Numbers (FCS_RNG)

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

Family behaviour:

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

Component levelling:

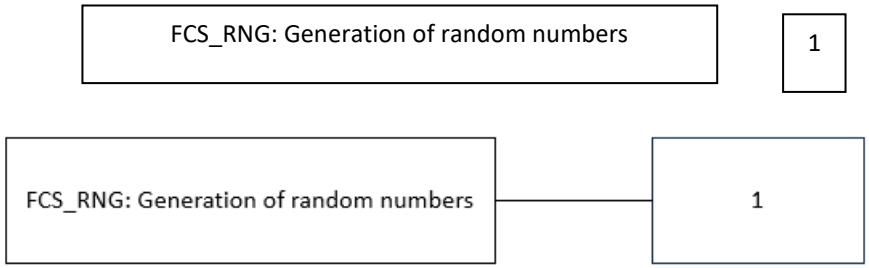

Fig 3. Component Leveling

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 22 (Application Note 29 from [5])

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 Use of requirement specifications

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each of these operations is used in this ST and the underlying PP. The footnotes in this ST indicate the operations of the PP and the ST as well.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements performed by the PP author is denoted as ***underlined italic bold text***. Refinement of security requirements performed by the ST author is denoted by **bold text**. Refinements by the ST author resulting in deleted text are indicated using ~~**strikethrough bold text.**~~ In addition, if the refinement performed by the ST author belongs to a selection or to an assignment that was performed by the PP author it is denoted as **underlined bold**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections filled in by the ST author are denoted as double underlined text and a foot note lists the selection choices from the PP.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. In some cases, the assignment made by the PP authors defines a selection to be performed by the ST author, this selection is denoted as *underlined and italicized text*. Assignments filled in by the ST author are denoted as double underlined text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

The formatting conventions that are used for the various operations are summarised in Table 6-1 for ease of reference.

Table 6-1: Operation formatting conventions

Operation	Performed by PP author	Performed by ST author
Refinement (general)	***Underlined italic bold text***	**Bold text**
Refinement (deletion)	-	~~**Strikethrough bold text**~~
Refinement of selection/assignment performed by PP author	-	**Underlined bold text**
Selection	Underlined text	Double underlined text
Assignment	Underlined text	Double underlined text
Assignment performed by PP author resulting in selection to be filled by ST author	-	*Underlined italicized text*

6.2 Subjects, Objects and Operations

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

Table 6-2 Subjects

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 6-3 Objects

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 6-4 Subjects, Objects and Operations

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

Subject	Operation	Object	Description
			privileged user.
R.Privileged_User	Create_New_Signer[2]	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	A key pair can be generated and

[2] To create a Signer the Authenticated Application (SSA) makes a call to the TOE containing the requisite objects, the TOE will acknowledge the operation and then the SSA will store the related objects. The objects are not stored persistently by the TOE.

Subject	Operation	Object	Description
		R.Signing_Key_Id	assigned to a signer.
R.Privileged_User ~~**R.Signer**~~[3]	Signer_Key_Pair_Deletion	R.Signer R.SVD R.Signing_Key_Id	A key pair can be deleted from a signer.
R.Privileged_User	Signer_Maintenance[4]	R.Signer R.Reference_Signer_Authentication_Data	Maintain the signer's security attributes.
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.

[3] The TOE does not allow Signer users to delete key pairs.
[4] To maintain a Signer the Authenticated Application (SSA) makes a call to the TOE containing the requisite objects, the TOE will acknowledge the operation and then the SSA will update the related objects in persistent storage. The objects are not stored persistently by the TOE.

Subject	Operation	Object	Description
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 SSA.
- FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 describes rules for creation, maintaining and usage of the R.Signer object as well as requirements to its values.

Authentication

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

Create Signer

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

Signer Key Pair Generation

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

Signer Key Pair Deletion

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

Signer Maintenance

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

Supply DTBS/R

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

Signing

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

Privileged User object

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

Privileged User Creation

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

TOE Maintenance

- FDP_ACC.1/TOE Maintenance using FDP_ACF.1/TOE Maintenance
- FMT_SMF.1, FMT_SMR.2 and FMT_MTD.1 requires the TOE to be able to carry out management functions and maintain users and roles.
- FPT_PHP.1 and FPT_PHP.3 requires the detection of any physical tampering or opening the case that compromises the TOE.

Audit

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

Communication

- FTP_TRP.1/SSA and FTP_TRP.1/SIC requires that either the Privileged User or the Signer initiates the communication.
- FCS_RNG.1 is required to generate random numbers for securing communication channels.
- FTP_ITC.1/CM requires trusted path for communication between SAM and the CM.

6.4 Security Functional Requirements

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

6.4.1 Security Audit (FAU)

FAU_GEN.1 Audit Generation	
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: - a) Start-up and shutdown of the audit functions; b) All auditable events for the not specified[5] level of audit; and

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

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;[6]

[6] [assignment: *other specifically defined auditable events*.]

k) none [7]

Application Note 23 (Application Note 28 from [5], refined by the ST Author).

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 should include failed verification of assertion provided by IdP or mobile application.

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

Application Note 24 (Application Note 29 from [5])

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

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

Application Note 25 (Application Note 30 in [5], refined by ST author)

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:

- Type of action performed (success or failure),

- identity of the role which performs the operation,
- unique log ID,
- readable message or status about the operation. [8]

Application Note 26 (Application Note 31 from [5], refined by the ST author)

Audit trail does 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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

[8] [assignment: *other audit relevant information*

FIA_UID.1 Timing of identification

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

6.4.2 Cryptographic Support (FCS)

FCS_CKM.1/RSA Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA[9] and specified cryptographic key sizes see Table 6-5[10] that meet the following: see Table 6-5[11]

FCS_CKM.1/AES Cryptographic key generation	
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or

[9] [assignment: *cryptographic key generation algorithm*]
[10] [assignment: *cryptographic key sizes*]
[11] [assignment: *list of standards*]

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm AES[12] and specified cryptographic key sizes see Table 6-5[13] that meet the following: see Table 6-5[14]

FCS_CKM.1/ECDSA Cryptographic key generation

Hierarchical to: No other components.

[12] [assignment: *cryptographic key generation algorithm*]
[13] [assignment: *cryptographic key sizes*]
[14] [assignment: *list of standards*]

Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ ECDSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDSA[15] and specified cryptographic key sizes see Table 6-5[16] that meet the following: see Table 6-5[17]

[15] [assignment: *cryptographic key generation algorithm*]
[16] [assignment: *cryptographic key sizes*]
[17] [assignment: *list of standards*]

Table 6-5 FCS_CKM.1 key generation parameters

Key Algo	Key Size	Standard
AES	256	SOG-IS [10]
RSA	2048, 3072, 4096	PKCS#1 [15] FIPS 186-5 [16] SOG-IS [10] ETSI TS 119 312[9]
ECDSA	192, 224, 256, 384 & 512	FIPS 186-5 [16] SOG-IS [10]ETSI TS 119 312[9] RFC 5639 [18] ANSI X9.62[18]

Application Note 27 (Application Note 32 from [5])

The TOE uses a CM certified in conformance with EN 419 221-5 [7]. See also OE.CRYPTOMODULE_CERTIFIED for key generation. Although the TSF may not generate keys itself, these FCS SFRs express the requirement for the TSF to invoke the CM with the appropriate parameters whenever key generation is required.

Guidance on cryptographic algorithms can be found in ETSI TS 119 312 [9] or SOG-IS [10]. This application note is applied to all three SFRs that are FCS_CKM.1/RSA, FCS_CKM.1/AES and FCS_CKM.1/ECDSA

Application Note 28 (Application Note 33 from [5])

The TOE uses Certified CM to generate cryptographic keys for different purposes, e.g., application, infrastructure, and session. The ST writer has included an iteration of this SFR for every key type it generates itself. This application note is applied to all three SFRs that are FCS_CKM.1/RSA, FCS_CKM.1/AES and FCS_CKM.1/ECDSA

FCS_CKM.4 Cryptographic key destruction	
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroise[18] that meets the following: FIPS 140-3 [17][19].

[18] [assignment: *cryptographic key destruction method*]

Application Note 29 (Application Note 34 from [5])

The TOE uses a CM certified in conformance with EN 419 221-5 [7] for key destruction. The Certified CM is responsible for all the infrastructure keys used by the TOE for their operations e.g., Encryption and HSM master key which is used by Certified CM to encrypt the key pairs generated for the signer user.

Application Note 30 (Application Note 35 from [5])

Zeroisation of the keys is the common method of the TOE. Certified CM performs the Zeroisation

FCS_COP.1/DIG_SIG_GEN Cryptographic operation

Hierarchical to: No other components.

[19] [assignment: *list of standards*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ DIG_SIG_GEN	The TSF shall perform digital signature – generation[20] in accordance with a specified cryptographic algorithm Table 6-6: Signature generation algorithm[21] and cryptographic key sizes Table 6-6: Key sizes[22] that meet the following: Table 6-6: Applicable standards[23].

[20] [assignment: *list of cryptographic operations*]
[21] [assignment: *cryptographic algorithm*]
[22] [assignment: *cryptographic key sizes*]
[23] [assignment: *list of standards*]

Table 6-6 Signature generation algorithm

Signature generation algorithm	Key sizes	Padding / Short curve name	Hash algorithm	Applicable standards
RSA	2048, 3072, 4096, bits	RSASSA-PKCS-v1.5 RSASSA-PSS	SHA-224, SHA256, SHA-384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	PKCS#1 [15] FIPS 186-5 [16] SOG-IS [10] ETSI TS 119 312[9]
ECDSA	192, 224, 256, 384, 521 bits	NIST P-256, P-384, P-521 **Brainpool** brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1	SHA-224, SHA256, SHA-384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5 [16] SOG-IS [10]ETSI TS 119 312[9] RFC 5639 [18] ANSI X9.62[18]

Application Note 31 (Application Note 36 from [5])

The TOE uses a CM certified in conformance with EN 419 221-5 [7] for cryptographic operations.

Application Note 32 (Application Note 37 from [5])

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 eIDAS Regulation No 910/2014 [8] and a list of approved signature and seal formats are given in [13].

Application Note 33 (Application Note 38 from [5])

Any algorithms that are not listed in Table 6-6 that are supported for backward compatibility and legacy applications in eTugra SAM are not in the scope of the ST.

If the TOE uses the aforementioned weaker algorithms, it is outside of the scope of this ST.

FCS_COP.1/DIG_SIG_VER Cryptographic operation	
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ DIG_SIG_VER	The TSF shall perform digital signature – verification[24] in accordance with a specified cryptographic algorithm Table 6-7: Signature verification algorithm[25] and cryptographic key sizes

[24] [assignment: *list of cryptographic operations*]
[25] [assignment: *cryptographic algorithm*]

Table 6-7: Key sizes[26] that meet the following: Table 6-7: Applicable standards[27].

Table 6-7 Signature verification algorithm

Signature verification algorithm	Key sizes	Padding / Short curve name	Hash algorithm	Applicable standards
RSA	2048, 3072, 4096bits	RSASSA-PKCS-v1.5 RSASSA-PSS	SHA224, SHA256, SHA384, SHA512, SHA3-224,	PKCS#1 [15] FIPS 186-5 [16] SOG-IS [10] ETSI TS 119 312[9]

[26] [assignment: *cryptographic key sizes*]
[27] [assignment: *list of standards*]

Signature verification algorithm	Key sizes	Padding / Short curve name	Hash algorithm	Applicable standards
			SHA3-256, SHA3-384, SHA3-512	
ECDSA	192, 224, 256, 384, 521 bits	NIST P-256, P-384, P-521 **Brainpool** brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1	SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 186-5 [16] SOG-IS [10]ETSI TS 119 312[9] RFC 5639 [18] ANSI X9.62[18]

FCS_COP.1/HASH Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

	FCS_CKM.1 Cryptographic key generation]
	FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ HASH	The TSF shall perform cryptographic hash function[28] in accordance with a specified cryptographic algorithm SHA256, SHA384, SHA512, SHA3-256, SHA3-384, SHA3-512 [29] and cryptographic key sizes none[30] that meet the following: ETSI TS 119 312 [9], FIPS 186-5 [16][31].

[28] [assignment: *list of cryptographic operations*]
[29] [assignment: *cryptographic algorithm*]
[30] [assignment: *cryptographic key sizes*]
[31] [assignment: *list of standards*]

FCS_COP.1/HMAC Cryptographic operation	
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ HMAC	The TSF shall perform keyed-hash message authentication code[32] in accordance with specified cryptographic algorithms HMAC-SHA256, HMAC-SHA384, HMAC-SHA-512[33] and

[32] [assignment: *list of cryptographic operations*]
[33] [assignment: *cryptographic algorithm*]

cryptographic key sizes: 512 bit (for HMAC-SHA256), 1024 bits (for HMAC-SHA384 and HMAC-SHA512)[34] that meet the following: RFC 6151 [19][35].

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

[34] [assignment: *cryptographic key sizes*]
[35] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ ENC	The TSF shall perform key encryption[36] in accordance with a specified cryptographic algorithm AES[37] and cryptographic key sizes 256bits[38] that meet the following: SOG-IS [10][39].

The next SFR is relevant when the TOE is deployed in an appliance distinct from the CM.

FCS_RNG.1 Generation of random numbers

Hierarchical to: No other components.

[36] [assignment: *list of cryptographic operations*]
[37] [assignment: *cryptographic algorithm*]
[38] [assignment: *cryptographic key sizes*]
[39] [assignment: *list of standards*]

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a deterministic[40] random number generator that implements: securing communication with CM[41].

FCS_RNG.1.2 The TSF shall provide bits[42] that meet BSI AIS 20/31 v2.0 [20] or NIST 800-90A [21] [43].

Application Note 34 (Application Note 38 from [5])

For more information on the selections and assignments, see the SFR definition in Clause 8.

[40] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*
[41] [assignment: *list of security capabilities*]
[42] [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
[43] [assignment: *a defined quality metric*]

Application Note 35 (Application Note 39 from [5])

The TOE communicates with the CM over secure channel which uses the deterministic random number generator.

Application Note 36 (Application Note 39 from [5])

The algorithm to be used can be configured, the available RNG algorithm configurations are: -

- HMAC/SHA-256 MAC-based secure random according to NIST SP800-90A; or
- SHA-256 hash-based secure random according to BSI AIS 20 v2.0.

6.4.3 User Data Protection (FDP)

Table 6-8 Privileged User Authorization

Role	Authorised operations
User Manager: Administrator	Privileged user creation TOE maintenance
User Manager: Security Officer	Privileged user creation TOE maintenance (Configuration approval)

Role	Authorised operations
Authenticated Application	Signer creation Signer maintenance Signer User key generation Signer User key deletion Supply DTBS/R Signing

Application Note 37 (Application Note 40 from [5])

The above User Authorization Table shows which roles are authorized to perform certain operations.

FDP_ACC.1/Privileged User Creation	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Privileged User Creation	The TSF shall enforce the Privileged User Creation SFP[44] on: - Subjects: Privileged User **(User Manager)** Objects: New security attributes for the Privileged User to be created.

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

Operations: Create New Privileged User:
The TOE creates R.Privileged User and R.Reference Privileged User Authentication Data with information transmitted by Privileged User.[45]

Application Note 38 (Application Note 40 from [5])

When eTugra SAM setup and initialized one User Manager 'administrator' is created. The administrator can create both User Managers operators and Authenticated Application (SSA) also.

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

Hierarchical to: No other components.

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

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Privileged User Creation	The TSF shall enforce the Privileged User Creation SFP[46] to objects based on the following: - 1) whether the subject is a Privileged User **(User Manager)** authorized to create a new Privileged User.[47]
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: -

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

1) Only a Privileged User **(User Manager)** who has been authorised for creation of new users can carry out the Create New Privileged User operation.[48]

FDP_ACF.1.3/ Privileged User Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None.[49]
FDP_ACF.1.4/ Privileged User Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: None.[50]

[48] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[49] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[50] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1/Signer Creation	Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signer Creation	The TSF shall enforce the Signer Creation SFP[51] on: - Subjects: Privileged User **(Authenticated Application)** 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 **(Authenticated Application)**[52]

[51] [assignment: *access control SFP*]
[52] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Application Note 39 (Application Note 40 from [5])

The Authenticated Application (SSA) makes a call to the TOE to trigger Signer creation, the TOE will acknowledge the operation and then the SSA will store the related objects persistently stored. The TOE does not store the related objects persistently.

FDP_ACF.1/Signer Creation	Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signer Creation	The TSF shall enforce the Signer Creation SFP[53] to objects based on the following: - 1) whether the subject is a Privileged User **(Authenticated Application)** authorized to create a new Signer.[54]
FDP_ACF.1.2/ Signer Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - 1) Only a Privileged User **(Authenticated Application)** who has been authorised for creation of new users can carry out the Create New Signer operation.[55]

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

FDP_ACF.1.3/ Signer Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules*:* None.[56]
FDP_ACF.1.4/ Signer Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: None.[57]

FDP_ACC.1/Signer Maintenance Subset access control	
Hierarchical to:	No other components.

[55] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[56] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[57] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signer Maintenance	The TSF shall enforce the Signer Maintenance SFP [58] on: - Subjects: Privileged User **(Authenticated Application)** ~~**and Signer**~~ Objects: The security attributes R.Reference_Signer_Authentication_Data of R.Signer Operations: Signer_Maintenance: The Privileged User **(Authenticated Application)** ~~**or Signer**~~ instructs the TOE to update R.Reference_Signer_Authentication_Data of R.Signer.[59]

[58] [assignment: *access control SFP*]
[59] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Application Note 40 (Application Note 40 from [5])

The Authenticated Application (SSA) makes a call to the TOE to trigger Signer maintenance e.g; update signer information, the TOE will acknowledge the operation and then the SSA will update the related objects in persistent storage. The TOE does not store the related objects persistently rather SSA maintains the signer users in its database, therefore TOE is not required to maintain signer user

FDP_ACF.1/Signer Maintenance Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signer Maintenance	The TSF shall enforce the Signer Maintenance SFP[60] to objects based on the following: 1) Whether the subject is a Privileged User **(Authenticated application)** ~~**or Signer**~~ authorised to maintain the Signer security attributes.[61]
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 **(Authenticated Application)** ~~**or Signer**~~ who has been authorised to maintain a Signer can

[60] [assignment: *access control SFP*]
[61] [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*]

carry out the Signer Maintenance operation.[62]

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.**~~ **None**[63]
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.[64]

[62] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[63] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[64] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Application Note 40a
Authenticated app (SSA) is first authenticated and authorised by TOE to request signer maintenance. Only authenticated application (SSA) can invoke signer user related operations. Signer user itself cannot maintain as signer user information is recorded by SSA. Any update in the signer user attributes is executed by SSA in its database after getting acknowledgement from TOE.

FDP_ACC.1/Signer Key Pair Generation Subset access control

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

FDP_ACC.1.1/ Signer Key Pair Generation	The TSF shall enforce the Signer Key Pair Generation SFP [65] on: - Subjects: Privileged User **(Authenticated Application)** ~~**and Signer**~~. Objects: The security attributes R.SVD and R.Signing Key Id as part of R.Signer. Operations: Generate Signer Key Pair: The Privileged User **(Authenticated application)** ~~**or Signer**~~ instruct the TOE to request the Cryptographic Module to generate a signing key pair R.Signing Key Id and R.SVD and assign them to the R.Signer. [66]

[65] [assignment: *access control SFP*]
[66] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Application Note 41 (Application Note 43 [5])

R.Authorisation_Data is generated by the TOE during signing key pair generation and bind together with R.Signing_Key_Id and R.SVD to be stored persistently in the Authenticated Application (SSA). Signer user cannot request key pair generation itself rather only authenticated application (SSA) can request TOE to generate signing key pair in the CM on behalf of signer user.

Application Note 42 (Application Note 42 from [5])

The R.Authorisation_Data are established as described in section 3.1. The signer's signing keys can be backed-up from one CM and imported to another CM.

Application Note 43 (Application Note 44 from [5])

Signing keys are generated on-demand for a specific signer, no auto-generated keys are used for signer.

Application Note 44 (Application Note 45 from [5])

The R.SVD is added to the CSR to get certificate from CA.

FDP_ACF.1/Signer Key Pair Generation Security attribute based access control	
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Signer Key Pair Generation	The TSF shall enforce the Signer Key Pair Generation SFP[67] to objects based on the following: - 1) whether the subject is a Privileged User **(Authenticated**

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

Application) ~~or Signer~~ authorised to generate a key pair.[68]

FDP_ACF.1.2/ Signer Key Pair Generation

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: -

1) Only a Privileged User **(Authenticated Application) ~~or Signer~~** who has been authorised to generate the key pair can carry out the Generate Signer Key Pair operation.[69]

FDP_ACF.1.3/

The TSF shall explicitly authorise access of subjects to objects

[68] [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*]

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

Signer Key Pair Generation	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.**~~**None**[70]
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. [71]

Application Note 45 (Application Note 46 from [5])

The Signer key pair generation operation can only be performed by the Privileged User (Authenticated Application (SSA)), and not the Signer user directly. The generated keys (R.SVD and encrypted private key), R.Signing_Key_Id and R.Authorisation_Data are stored

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

persistently by the Authenticated Application (SSA). The TOE does not store the related data persistently, the generated key pair is encrypted by HSM master key and exported from CM. The exported encrypted key pair is stored in the SSA database.

Application Note 46 (Application Note 46 from [5])

The TOE does not use pre-generated keys.

Application Note 47 (Application Note 47 from [5])

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

FDP_ACC.1/Signer Key Pair Deletion	Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Signer Key Pair Deletion	The TSF shall enforce the Signer Key Pair Deletion SFP [72] on: - Subjects: Privileged User **(Authenticated Application)** ~~**and Signer**~~ Objects: The security attributes R.Signing_Key_Id and R.SVD of R.Signer Operations: Signer_Key_Pair_Deletion: The Privileged User **(Authenticated Application)** ~~**or Signer**~~ instructs the TOE to delete the R.Signing_Key_Id and R.SVD from R.Signer.[73]

[72] [assignment: *access control SFP*]
[73] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Application Note 48 (Application Note 48 from [5])

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.

Signer user key pair is stored in SSA database in encrypted format (HSM master performs the encryption). The Authenticated Application (SSA) makes a call to the TOE to trigger Signer key pair deletion, the TOE will acknowledge the operation and then the SSA will delete the related encrypted key pair objects from persistent storage. The TOE does not store the related objects persistently.

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signer Key Pair Deletion	The TSF shall enforce the Signer Key Pair Deletion SFP [74] to objects based on the following: - 1) Whether the subject is a Privileged User **(Authenticated Application)** ~~**or Signer**~~ authorised to delete the Signer security attributes. [75]
FDP_ACF.1.2/ Signer Key Pair Deletion	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - 1) Only a Privileged User **(Authenticated Application)** ~~**or**~~

[74] [assignment: *access control SFP*]
[75] [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**~~ who has been authorised to delete a key pair can carry out the Signer Key Pair Deletion operation. [76]
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.**~~None[77]
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. [78]

[76] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[77] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

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

Application Note 48a
Authenticated application (SSA) is authenticated and authorised before signer key pair deletion along with R.SVD is deleted. SSA makes a call to TOE and after getting the acknowledgement, it deletes the signer key pair and R.SVD from its database. Signer user itself cannot perform this operation as SSA is responsible for this task on behalf of signer user.

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

FDP_ACC.1/Supply DTBS/R	Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Supply DTBS/R	The TSF shall enforce the Supply DTBS/R SFP[79] on: - Subjects: Privileged User **(Authenticated Application)** Objects: The security attributes R.DTBS/R of R.Signer. Operations: Supply DTBS/R: The Privileged User **(Authenticated Application)** instructs the TOE to link the supplied DTBS/R(s) to the next signature operation for R.Signer.[80]

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

FDP_ACF.1/Supply DTBS/R	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Supply DTBS/R	The TSF shall enforce the Supply DTBS/R SFP[81] to objects based on the following: - 1) Whether the subject is a Privileged User **(Authenticated**

[80] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[81] [assignment: *access control SFP*]

Application) authorised to supply a DTBS/R(s).[82]

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 **(Authenticated Application)** who has been authorised to supply a DTBS/R(s) can carry out the Supply DTBS/R operation.[83]
FDP_ACF.1.3/ Supply DTBS/R	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None.[84]

[82] [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*]
[83] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[84] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

FDP_ACF.1.4/ Supply DTBS/R	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None.[85]

FDP_ACC.1/Signing	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signing	The TSF shall enforce the Signing SFP [86] on: - Subjects: Signer Objects: R.Authorisation Data security attributes,

[85] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[86] [assignment: *access control SFP*]

R.Signing_Key_Id and R.DTBS/R of R.Signer and R.Signature.
Operations: Signing:
The Signer instructs the TOE to perform a signature operation containing the following steps:

- The TOE establishes R.Authorisation Data for the R.Signing_Key_Id.
- The TOE uses the R.Authorisation Data and R.Signing_Key_Id to activate a signing key in the Cryptographic Module and signs the R.DTBS/R resulting in R.Signature.
- The TOE deactivates the signing key when the signature operation is completed.[87]

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

Application Note 49 (Application Note 51 from [5])

R.Authorisation_Data (passphrase) and the encrypted CM signing key blob (which contains the R.SVD and the private signing key encrypted with the HSM master key) and R.Signing_Key_Id protected in both integrity and confidentiality are sent to the TOE by the SSA during signing. The TSF activates the signing key by decrypting R.Authorisation_Data and loading the CM signing key blob 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 (Application Note 52 from [5])

The Business Application (SCA) provides the document hash, i.e. DTBS/R, to SSA which passes it to the TOE for signature computation.

Application Note 51 (Application Note 53 from [5])

Signing key deactivation means that the Signer shall be required to re-authorise any subsequent use of it.

FDP_ACF.1/Signing	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Signing	The TSF shall enforce the Signing SFP [88] to objects based on the following: - 1) Whether the subject is a Signer authorised to create a signature. [89]

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

FDP_ACF.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. [90]

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. [91]

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

[90] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[91] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

used to create a signature. [92]

Application Note 52 (Application Note 54 from [5])

In FDP_ACF.1.2/Signing the default R.Signing_Key_Id can be implied.

FDP_ACC.1/TOE Maintenance	Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ TOE	The TSF shall enforce the TOE Maintenance SFP [93] on: Subjects: Privileged User **(User Manager)**

[92] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[93] [assignment: *access control SFP*]

Maintenance	Objects: R.TSF_DATA. Operations: TOE_Maintenance: The Privileged User **(User Manager)** transmits information to the TOE to manage R.TSF_DATA.[94]

FDP_ACF.1/TOE Maintenance	Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/	The TSF shall enforce the TOE_Maintenance_SFP [95] to objects

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

TOE Maintenance	based on the following: *1)* Whether the subject is a Privileged User **(User Manager)** authorised to maintain the TOE configuration data. [96]
FDP_ACF.1.2/ TOE Maintenance	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - 1) Only a Privileged User **(User Manager)** who has been authorised to maintain the TOE can carry out the TOE Maintenance operation. [97]

[95] [assignment: *access control SFP*]
[96] [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*]
[97] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP_ACF.1.3/ TOE Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: None. [98]
FDP_ACF.1.4/ TOE Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: None. [99]

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

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

FDP_ETC.2/Signer	Export of user data with security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
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 [100] when exporting user data, controlled under the SFP(s), outside of the TSF.
FDP_ETC.2.2/	The TSF shall export the user data with the user data's

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

Signer	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. [101]

[101] [assignment: *additional exportation control rules*]

Application Note 53 (Application Note 55 from [5])

The TOE exports the following user data:

During Signer Key Pair Generation:

- The encrypted CM signing key blob (which contains the R.SVD and the private signing key encrypted with the HSM master key) is transmitted to the SSA for storage

Note that data exchanged between the TOE and the CM are not included, as even though the TOE is not installed in the CM, the TOE and the CM are still contained within the same tamper protected physical boundary.

FDP_IFC.1/Signer	Subset information flow control

Hierarchical to: No other components.

Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/ Signer	The TSF shall enforce the Signer Flow SFP [102] on Privileged User **(Authenticated Application)** ~~**and Signer**~~ accessing Signer security attributes for all operations. [103]

Application Note 53a
Signer user information is recorded into SSA database. SSA is authenticated and authorised before signer user security attributes are changed. SSA makes a call to TOE and after getting the acknowledgement, it updated the related security attributes of the signer user into its database against the signer user record. Signer user itself cannot perform this operation as SSA is responsible for this task on behalf of signer user.

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

FDP_IFF.1/Signer	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control, or FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/ Signer	The TSF shall enforce the Signer Flow SFP [104] based on the following types of subject and information security attributes: - Privileged User **(Authenticated Application)** ~~**and Signer**~~ accessing the Signer security attributes. [105]
FDP_IFF.1.2/	The TSF shall permit an information flow between a controlled

[104] [assignment: *information flow control SFP*]
[105] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

Signer	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. [106]
FDP_IFF.1.3/	The TSF shall enforce the: None. [107]

[106] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[107] [assignment: *additional information flow control SFP rules*]

Signer	
FDP_IFF.1.4/ Signer	The TSF shall explicitly authorise an information flow based on the following rules: None. [108]
FDP_IFF.1.5/ Signer	The TSF shall explicitly deny an information flow based on the following rules: None. [109]

Application Note 53b

Signer user cannot perform key pair generation, key pair deletion and signing operations rather SSA is doing this job on behalf of signer. TOE must be initialized and configured before SSA makes calls to TOE for the above operations. In Signing, SAD must be verified before TOE invokes CM to perform signature operation using the signer user key.

[108] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[109] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

FDP_ETC.2/Privileged User	Export of user data with security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/ Privileged User	The TSF shall enforce the Privileged User Creation SFP [110] 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.

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

FDP_ETC.2.3/ Privileged User	The TSF shall ensure that the security attributes, when exported outside the TSF, are unambiguously associated with the exported user data.
FDP_ETC.2.4/ Privileged User	The TSF shall enforce the following rules when user data is exported from the TSF: None. [111]

Application Note 54 (Application Note 55 from [5])

During Privileged user creation the TOE exports the R.Reference_Privileged_User_Authentication_Data to be stored in the RDBMS.

[111] [assignment: *additional exportation control rules*]

FDP_IFC.1/Privileged user	Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/ Privileged User: The TSF shall enforce the Privileged User Flow SFP [112] on Privileged User **(User Manager)** accessing Privileged User security attributes for all operations. [113]

FDP_IFF.1/Privileged User	Simple security attributes

Hierarchical to: No other components.

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

Dependencies:	FDP_IFC.1 Subset information flow control, or FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/ Privileged User	The TSF shall enforce the Privileged User Flow SFP[114] based on the following types of subject and information security attributes: - Privileged User **(User Manager)** accessing the Privileged User security attributes.[115]
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: -

[114] [assignment: *information flow control SFP*]
[115] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

	The TOE shall be initialized with FDP_ACC.1/TOE Maintenance.[116]
FDP_IFF.1.3/ Privileged User	The TSF shall enforce the: None.[117]
FDP_IFF.1.4/ Privileged User	The TSF shall explicitly authorise an information flow based on the following rules: None. [118]
FDP_IFF.1.5/ Privileged User	The TSF shall explicitly deny an information flow based on the following rules: None. [119]

[116] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[117] [assignment: *additional information flow control SFP rules*]
[118] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[119] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF Trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/	The TSF shall enforce the Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion, Signer Maintenance

Signer	SFP, Supply DTBS/R SFP and Signing SFP[120] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/ Signer	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/ Signer	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/ Signer	The TSF shall ensure that interpretation of the security attributes of the imported user data are as intended by the source of the user data.
FDP_ITC.2.5/	The TSF shall enforce the following rules when importing user

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

Signer	data controlled under the SFP from outside the TOE: None. [121]

[121] [assignment: *additional importation control rules*]

Application Note 55 (Application Note 57 from [5])

The TOE imports the following data:

During Signer Creation:

- R.Signer (contains signer identifier only)
- R.Reference_Signer_Authentication_Data

During Signer key pair generation:

- R.Authorisation_Data

During Signer key pair deletion:

- R.Signing_Key_Id

During Signer Maintenance:

- R.Signer (contains signer identifier only)
- R.Reference_Signer_Authentication_Data

During Supply DTBS/R:

- R.DTBS/R

During Signing:

- Encrypted CM signing key blob (contains R.SVD and private signing key encrypted with HSM master key)
- R.SAD which includes:
    - R.Signing_Key_Id
    - R.DTBS/R
    - IdP/SIC assertion
- R.Authorisation_Data

Note that data exchanged between the TOE and the CM is not considered because they lie within the same tamper protected environment.

FDP_ITC.2/Privileged User	Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF Trusted channel, or

FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/ Privileged User	The TSF shall enforce the Privileged User Creation SFP [122] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/ Privileged User	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/ Privileged User	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/ Privileged User	The TSF shall ensure that interpretation of the security attributes of the imported user data are as intended by the source of the user data.
FDP_ITC.2.5/ Privileged User	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: None. [123]

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

Application Note 56 (Application Note 58 from [5])

The TOE imports the following data:

During Privileged User Creation:

- R.Privileged_User
- R.Reference_Privileged_User_Authentication_Data

FDP_UCT.1	Basic data exchange confidentiality

Hierarchical to: No other components.

[123] [assignment: *additional importation control rules*]

Dependencies:	[FTP_ITC.1 Inter-TSF Trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the Signer Flow SFP and Privileged User Flow SFP [124] to transmit and receive [125] user data in a manner protected from unauthorised disclosure.

[124] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[125] [selection: *transmit, receive]*

FDP_UIT.1	Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF Trusted channel, or

FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the Signer Flow SFP and Privileged User Flow SFP[126] **to be able to** transmit and receive[127] user data in a

[126] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[127] [selection: *transmit, receive*]

	manner protected from modification and insertion[128] errors **for R.Signer and R.Privileged User and for R.SAD also**[129] from *modification and replay*[130] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion[131] **for R.Signer and R.Privileged_User and for R.SAD**[132] whether *modification and replay*[133] has occurred.

[128] [selection: *modification, deletion, insertion, replay*]
[129] [selection: *modification, deletion, insertion, replay*]
[130] [selection: *modification, deletion, insertion, replay*]
[131] [selection: *modification, deletion, insertion, replay*]
[132] [selection: *modification, deletion, insertion, replay*]
[133] [selection: *modification, deletion, insertion, replay*]

Application Note 57 (Application Note 59 from [5])

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

6.4.4 Identification & Authentication (FIA)

FIA_AFL.1/SSA	Authentication failure handling
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 / SSA	The TSF shall detect when a TOE Maintenance configurable positive within 5[134] unsuccessful authentication attempts occur related to Privileged User **(Authenticated Application)** ~~**and**~~

[134] [selection: *[assignment: 5], a TOE Maintenance configurable positive within [assignment: 5 to 10]]*

	~~**Signer**~~ authentication.[135]
FIA_AFL.1.2 / SSA	When the defined number of unsuccessful authentication attempts has been met[136], the TSF shall suspend the Privileged User **(Authenticated Application) which marks it inactive** ~~**and when it is a Signer suspend the usage of R.Signing_Key_Id**~~[137]

Application Note 58 (Application Note 60 from [5])

The TOE checks the unsuccessful authentication attempts made by the Authenticated Application (SSA) and in case the limit is exceeded, the TOE marks the SSA as inactive. The default value of the configurable unsuccessful authentications limit is 5.

[135] [assignment: *list of authentication events*]
[136] [selection: *met, surpassed*]
[137] [assignment: *list of actions*]

FIA_AFL.1/User Manager	Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 User Manager	The TSF shall detect when a TOE Maintenance configurable positive within 5[138] unsuccessful authentication attempts occur related to Privileged User **(User Manager Operator)** ~~**and Signer**~~ authentication.[139]
FIA_AFL.1.2 / User Manager	When the defined number of unsuccessful authentication attempts has been met[140], the TSF shall suspend the Privileged User **(User Manager Operator) which marks it inactive** ~~**and**~~

[138] [selection: *[assignment: 5], a TOE Maintenance configurable positive within [assignment: 5 to 10]]*
[139] [assignment: *list of authentication events*]
[140] [selection: *met, surpassed*]

~~when it is a Signer suspend the usage of R.Signing_Key_Id~~[141]

Application Note 59a (Application Note 60 from [5])

The TOE checks the unsuccessful authentication attempts made by the User Manager Operator and in case the limit is exceeded, the TOE marks the User Manager Operator as inactive. The default value of the configurable unsuccessful authentications limit is 5.

[141] [assignment: *list of actions*]

Application Note 60 (Application Note 60 from [5])

Signers are authenticated by delegated authentication by an IdP or a mobile application via SSA. It is the responsibility of the IdP or mobile application to detect failed authentication and suspend signer users. TOE doesn't support direct authentication, therefore the SFR does not apply and is trivially fulfilled.

FIA_ATD.1	User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: the security attribute as defined in FIA_USB.1.142

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

FIA_UAU.2	User authentication before any action
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 61 (Application Note 61 from [5]) The TOE only supports indirect authentication. The TOE considers a signer user to be authenticated when an assertion/signature has been validated.

FIA_UAU.5/Signer	Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/ Signer ***The TSF shall provide delegated authentication based on IdP or mobile application assertion where the IdP or mobile application follows the guidelines defined in eIDAS regulation EN 419 241-1 [6][143] to support Signer authentication[144].***

[143] [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]*]

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

FIA_UAU.5.2/ Signer	***The TSF shall authenticate any Signer's claimed identity according to: verification of an IdP or mobile application assertion***[145]

Application Note 62 (Application Note 62 from [5])

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

The authentication factors used to authenticate the signer are managed by the IdP or mobile application via SSA and are thus out of scope of this ST.

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

Successful authentication gives Signer access to the relevant R.Signer object as the owner. Before signing, SAD is verified in integrity. R.SAD is verified that it binds together the signer authentication, a set of R.DTBS/R and R.Signing_Key_Id. The R.DTBS/R used for signature operations is bound to the R.SAD. The authenticated signer user assertion is signed by IdP through asymmetric keys. TOE verifies the received signed assertion cryptographically through IdP assertion certificate and also matches the Signer Id in the assertion.

FIA_UAU.5/Privileged User	Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/ Privileged User	The TSF shall provide: - 1) The authentication of the Authenticated Application is

done using OAuth client credentials workflow

2) User name and password based authentication over OAuth is performed for User Manager;[146]

to support ***Privileged User*** authentication.

FIA_UAU.5.2/ Privileged User	The TSF shall authenticate any **Privileged User's** claimed identity according to the OAuth client credentials flow[147]

Application Note 61a

SSA as authenticated application uses OAuth client credentials flow by providing Client ID/Secret and after successful authentication OAuth token is being granted and SSA is authorised to perform signer user operations. Similarly user manager provides credentials and after

[146] [assignment: *list of authentication mechanisms*]
[147] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

successful authentication an OAuth token is granted and user manager is authorised to perform TOE configurations using Administration APIs.

FIA_UID.2	User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: No dependencies.

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

FIA_USB.1	User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition.

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

1) R.Reference_Signer_Authentication_Data;
2) R.Signing_Key_Id;
3) R.SVD;
4) R.Signer; and

5) R.Authorisation_Data[148]

to Signer: -

1) R.Reference_Privileged_User_Authentication_Data; and

2) R.Privileged_User[149]

to Privileged User.[150]

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

1) Whether the subject is a Privileged User **(Authenticated**

[148] [assignment: *list of user security attributes*]
[149] [assignment: *list of user security attributes*]
[150] [assignment: *list of user security attributes*]

Application) authorized to create a new Signer.

2) Whether the subject is a Privileged User **(User Manager)** authorized to create a new Privileged User **(Authenticated Application or User Manager)**.

3) None [151] *152*

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 **(Authenticated Application, User Manager)** authorized to modify an

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

R.Signer object.

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

3) None [153] [154]

Application Note 63 (Application Note 63 from [5])

In FIA_USB.1.2 several attributes including R.Signing_Key_Id, R.SVD and R.DTBS/R may initially be empty. SSA is authenticated and authorised to request signer operations, signer itself cannot modify its signer as SSA is authorised to do this job on behalf of signer user.

Application Note 64 (Application Note 65 from [5])

The Business Application (SCA) provides the document hash (DTBS/R) to SSA which passes it to the TOE for signature computation.

[153] [assignment: *rules for the changing of attributes*]
[154] [assignment: *rules for the changing of attributes*]

Application Note 65 (Application Note 64 from [5])

The R.Authrorisation_Data as a security can only be maintained by the Privileged User, and not the Signer, therefore the relevant part of the SFR is trivially satisfied.

6.4.5 Security Management (FMT)

FMT_MSA.1/Signer	Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ Signer	The TSF shall enforce the: - 1) Signer Creation SFP [155] to restrict the ability to create [156] the security attributes listed in FIA_USB.1 for Signer [157] to authorised Privileged User **(Authenticated Application)** [158]. 2) Generate Signer Key Pair SFP [159] to restrict the ability to generate [160] the security attributes R.SVD and

[155] [assignment: *access control SFP(s), information flow control SFP(s)]*
[156] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[157] [assignment: *list of security attributes*]
[158] [assignment: *the authorised identified roles*]
[159] [assignment: *access control SFP(s), information flow control SFP(s)]*
[160] [selection: *change_default, query, modify, delete, [assignment: other operations]]*

R.Signing Key Id **as part of R.Signer** [161] to authorised Privileged User **(Authenticated Application)** ~~**and Signer**~~ [162].

3) Signer Key Pair Deletion SFP [163] to restrict the ability to destruct [164] the security attribute R.SVD and R.Signing Key Id as part of R.Signer [165] to authorised **Privileged User (Authenticated Application, User Manager)** ~~**Signer**~~. [166]

[161] [assignment: *list of security attributes*]
[162] [assignment: *the authorised identified roles*]
[163] [assignment: *access control SFP(s), information flow control SFP(s)]*
[164] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[165] [assignment: *list of security attributes*]
[166] [assignment: *the authorised identified roles*]

4) Supply DTBS/R SFP [167] to restrict the ability to create [168] the security attribute R.DTBS/R as part of R.Signer [169] to authorised Privileged User **(Authenticated Application)** [170].

5) Signing SFP [171] to restrict the ability to create [172] the security attribute R.DTBS/R as part of R.Signer [173] to authorised Signer. [174]

[167] [assignment: *access control SFP(s), information flow control SFP(s)]*
[168] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[169] [assignment: *list of security attributes*]
[170] [assignment: *the authorised identified roles*]
[171] [assignment: *access control SFP(s), information flow control SFP(s)]*
[172] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[173] [assignment: *list of security attributes*]
[174] [assignment: *the authorised identified roles*]

6) Signing SFP [175] to restrict the ability to query [176] the security attributes as listed in FIA USB.1 [177] to authorised Signer. [178]

7) Signer Maintenance SFP [179] to restrict the ability to change [180] the security attributes R.Reference Signer Authentication Data [181] to authorised Privileged User **(Privileged User) ~~and Signer~~**.

[175] [assignment: *access control SFP(s), information flow control SFP(s)]*
[176] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[177] [assignment: *list of security attributes*]
[178] [assignment: *the authorised identified roles*]
[179] [assignment: *access control SFP(s), information flow control SFP(s)]*
[180] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[181] [assignment: *list of security attributes*]

182

Application Note 64a
Signer user cannot perform key pair generation, key pair deletion and signing operations rather SSA is doing this job on behalf of signer. TOE must be initialized and configured before SSA makes calls to TOE for the above operations. In Signing, SAD must be verified before TOE invokes CM to perform signature operation using the signer user key. During Signing SSA provides the DTBS/R, signature authentication i.e. assertion and Key ID to TOE at the time of signature operation, after SAD verification by TOE, signature operation is performed by CM.

FMT_MSA.1/Privileged User	Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or

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

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ Privileged User	The TSF shall enforce the: - 1) Privileged User Creation SFP [183] to restrict the ability to create and query [184] the security attributes listed in FIA_USB.1 for Privileged User [185] to authorised Privileged User (**User Manager Security Officer /**

[183] [assignment: *access control SFP(s), information flow control SFP(s)]*
[184] [selection: *change_default, query, modify, delete, [assignment: other operations]]*
[185] [assignment: *list of security attributes*]

Administrator). [186]

FMT_MSA.2	Secure security attributes
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for all

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

security attributes listed in FIA_USB.1. [187]

FMT_MSA.3/Signer	Static attribute initialisation
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/ Signer	The TSF shall enforce the Signer Creation SFP [188] to provide restrictive [189] default values for security attributes that are used to enforce the SFP.

[187] [assignment: *list of security attributes*]
[188] [assignment: *access control SFP, information flow control SFP*]
[189] [*selection, choose one of: restrictive, permissive, [assignment: other property]]*

FMT_MSA.3.2/ Signer	The TSF shall allow the Privileged User **(Authenticated Application)** [190] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Privileged User	Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1/ Privileged User	The TSF shall enforce the Privileged User Creation SFP [191] to provide restrictive [192] default values for security attributes that

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

	are used to enforce the SFP.
FMT_MSA.3.2/ Privileged User	The TSF shall allow the Privileged User **(User Manager)** [193] to specify alternative initial values to override the default values when an object or information is created.

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

[191] [assignment: *access control SFP, information flow control SFP*]
[192] [*selection, choose one of: restrictive, permissive, [assignment: other property]]*
[193] [assignment: *the authorised identified roles*]

FMT_MTD.1.1 The TSF shall restrict the ability to: -

1) modify [194] the R.TSF_DATA data [195] to Privileged User **(User Manager)**. [196]

Application Note 66 (Application Note 66 from [5])

The TSF data includes configuration of User Manager: administrator roles.

FMT_SMF.1	Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

[194] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*
[195] [assignment: *list of TSF data*]
[196] [assignment: *the authorised identified roles*]

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; and
4) None. [197] [198]

FMT_SMR.2	Restrictions on security roles

Hierarchical to: FMT_SMR.1 Security roles

[197] [assignment: *additional list of management functions to be provided by the TSF*]
[198] [assignment: *list of management functions to be provided by the TSF*]

Dependencies: FIA_UTD.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: Signer and Privileged User **(User Manager and Authenticated Application)**[199], none. [200]

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[201] are satisfied.

Application Note 67 (Application Note 67 from [5])

A user having User Manager: administrator or security officer role has the role privileged user and similarly authenticated application (SSA) has privileged user role

[199] [assignment: *authorised identified roles*]
[200] [assignment: *other authorised identified roles*]
[201] [assignment: *conditions for the different roles*]

6.4.6 Protection of the TSF (FPT)

FPT_PHP.1	Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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 68 (Application Note 68 from [5])

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 [22] for Security Level 3.

FPT_PHP.3	Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1	TSF shall resist opening the case [202] to the cover [203] by responding automatically such that the SFRs are always enforced.

Application Note 69 (Application Note 69 from [5])

The TOE is contained within the same tamper protected hardware as the CM, however, the TOE is not implemented as a local application within the physical boundary of the CM. To make it clearer: the CM has its own tamper protection but the TOE is not implemented inside the CM. If the appliance detects tamper it zeroize itself i.e. trigger the tamper detection switch of the HSM which erase its keys.

Application Note 70 (Application Note 70 from [5])

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 [22] Security Level 3. As in the case of FPT_PHP.1, because

[202] [assignment: *physical tampering scenarios*]
[203] [assignment: *list of TSF devices/elements*]

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 [22] for Security Level 3.

FPT_RPL.1	Replay detection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: R.SAD. [204]

FPT_RPL.1.2 The TSF shall perform reject the signature operation [205] when replay is detected.

[204] [assignment: *list of identified entities*]

FPT_STM.1	Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[205] [assignment: *list of specific actions*]

Application Note 71 (Application Note 71 from [5])

TOE gets the time source using Fortigate, it gets authenticated via Active Directory and gets the authentication token. TOE then connects with the Fortigate on a particular port through certificate-based authentication. If authentication is successful, the communication is done via a secure channel. Fortigate communicates with multiple NTP Servers, picks the most accurate time and provides it to TOE.FPT_TDC.1

Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

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; and
7) R.Reference Privileged User Authentication Data
8) R.TSF DATA. [206]

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 [207] when interpreting the TSF data from another trusted IT product.

[206] [assignment: *list of TSF data types*]

Application Note 72 (Application Note 72 from [5])

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

6.4.7 Trusted Paths/Channels (FTP)

FTP_TRP.1/SSA	Trusted path
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1/ SSA	The TSF shall provide a communication path between itself and: ***Privileged User*** **(User Manager and Authenticated Application)**

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

	~~through SSA~~[208] 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. [209]
FTP_TRP.1.2/ SSA	The TSF shall permit: ***Privileged User*** **(User manager and Authenticated Application) ~~through SSA~~** [210] 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;

[208] [selection: *remote, local]*
[209] [selection: *modification, disclosure, [assignment: other services for which trusted path is required]]*
[210] [selection: *the TSF, local users, remote users*]

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. [211] [212]

Application Note 73 (Application Note 73 from [5])

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. Application Note 15 from PP states that Privileged Users can interact with the TOE directly or via the SSA. Based on this

[211] [assignment: *other services for which trusted path is required*]
[212] [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

statement User manager communicates directly with TOE over secure TLS channel by providing credentials using OAuth protocol and authorised to perform TOE configurations. Similarly, all the signer user operations (signer key pair generation, key pair deletion and signing) are managed by SSA on behalf of signer user.

FTP_TRP.1/SIC	Trusted path
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1/ SIC	The TSF shall provide a communication path between itself and: ***Remote Signer through the SIC***[213] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the

[213] [selection: *remote, local]*

	communicated data from modification. [214]
FTP_TRP.1.2/ SIC	The TSF shall permit: ***Remote Signer through the SIC***[215] 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 [216] [217]

[214] [selection: *modification, disclosure, [assignment: other services for which trusted path is required]]*
[215] [selection: *the TSF, local users, remote users*]
[216] [assignment: *other services for which trusted path is required*]
[217] [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

Application Note 74 (Application Note 74 from [5])

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.

FTP_ITC.1/CM	Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/ CM	The TSF shall provide a communication path between itself and a ***CM certified according to EN 419 221-5 [7]*** 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 CM certified according to EN 419 221-5 [7]*** [218] to initiate communication via the trusted channel.
FTP_ITC.1.3/ CM	The TSF shall initiate communication via the trusted channel for all functions which need a CM. [219]

Application Note 75 (Application Note 75 from [5])

Communication with the CM is through a secure channel in any case.

[218] [selection: *the TSF, another trusted IT product*]
[219] [assignment: *list of functions for which a trusted channel is required*]

6.5 Security Requirements Rationale

6.5.1 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.

Table 6-9 Security requirements coverage

	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							

	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
FAU_GEN.2										X							
Cryptographic Support																	
FCS_CKM.1/RSA			X													X	
FCS_CKM.1/ECDSA			X													X	
FCS_CKM.1/AES			X													X	
FCS_CKM.4			X														
FCS_COP.1/															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
DIG_SIG_GEN																	
FCS_COP.1 /DIG_SIG_VER															X	X	
FCS_COP.1/HASH															X	X	
FCS_COP.1/HMAC							X		X							X	
FCS_COP.1/ENC			X													X	
FCS_RNG.1			X														X
User Data Protection																	

	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
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_ACF.1/Signer		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
Maintenance																	
FDP_ACC.1/Signer Maintenance		X						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									

	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
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									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/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/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_IFF.1/Privileged User					X		X										
FDP_ITC.2/Signer	X																
FDP_ITC.2/Privileged User					X		X										
FDP_UCT.1	X																
FDP_UIT.1	X																
Identification and																	

	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
Authentication																	
FIA_AFL.1/SSA						X					X						
FIA_AFL.1/User Manager						X											
FIA_ATD.1	X				X		X										
FIA_UAU.2						X					X						
FIA_UAU.5/Signer											X						
FIA_UAU.5/Privileged User						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
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									

	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
FMT_MSA.3/Signer								X									
FMT_MSA.3/Privileged User					X			X									
FMT_MTD.1									X								
FMT_SMF.1									X								
FMT_SMR.2									X								
Protection of the TSF																	

	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
FPT_PHP.1									X								
FPT_PHP.3									X								
FPT_RPL.1												X					
FPT_STM.1										X							
FPT_TDC.1	X				X		X										
Trusted Path/Channels																	
FTP_TRP.1/SSA									X					X			

	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
FTP_TRP.1/SIC												X	X	X			
FTP_ITC.1/CM			X												X		

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.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_Authentication_Data.

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

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

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). The actual description of the data is described in FIA_ATD.1 and FIA_USB.1. Authentication of Privileged User is handled by FIA_UID.2, FMT_MSA.1/Privileged User, FMT_MSA.2 and FMT_MSA.3/Privileged User. FDP_ACC.1/Privileged User Creation and FDP_ACF.1/Privileged User Creation describes access controls for creating Privileged Users.

OT.PRIVILEGED_USER_AUTHENTICATION is handled by FIA_AFL.1/SSA, FIA_AFL.1/User Manager, FIA_UAU.2 and FIA_UAU.5/Privileged User.

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

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, FDP_ACF.1/Signer Maintenance, FDP_ACC.1/Signer Key Pair Deletion and FDP_ACF.1/Signer Key Pair Deletion. 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. FTP_TRP.1/SSA describes that only a Privileged User can maintain a 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.

OT.SAD_VERIFICATION is handled by the FIA_AFL.1/SSA, FIA_UAU.2 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. Also covered by access control rules FDP_ACC.1/Supply DTBS/R and FDP_ACF.1/Supply DTBS/R for transmitting DTBS/R to the TSF.

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

OT.CRYPTO is covered by FCS_CKM.1/RSA, FCS_CKM.1/ECDSA, FCS_CKM.1/AES, FCS_COP.1/DIG_SIG_GEN, FCS_COP.1/DIG_SIG_VER, FCS_COP.1/HASH, FCS_COP.1/HMAC, FCS_COP.1/ENC, which describes requirements for key generation and algorithms.

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

6.6 SFR Dependencies

The dependencies between SFRs are addressed as shown in Table 6-10.

Table 6-10 Dependencies

Requirement	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DIG_SIG_GEN, FCS_COP.1/DIG_SIG_VER, and FCS_CKM.4
FCS_CKM.1/ECDSA	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/DIG_SIG_GEN, FCS_COP.1/DIG_SIG_VER, and FCS_CKM.4
FCS_CKM.1/AES	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/ENC, and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/*
FCS_COP.1/DIG_SIG_GEN	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.1/ECDSA and FCS_CKM.4
FCS_COP.1/DIG_SIG_VER	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.1/ECDSA and FCS_CKM.4

Requirement	Dependencies	Fulfilled by
FCS_COP.1/HASH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not fulfilled[220]
FCS_COP.1/HMAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.1/ECDSA and FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/AES and FCS_CKM.4

[220] The dependencies of FCS_COP.1 for Cryptographic key management (key import or generation and key destruction) are not needed for the */Hash iteration as the Cryptographic hash operation does not require the use of a Cryptographic key value.

Requirement	Dependencies	Fulfilled by
FCS_RNG.1	None	No dependents
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 Key Pair Generation	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Generation
FDP_ACC.1/Signer Maintenance	FDP_ACF.1	FDP_ACF.1/Signer Maintenance
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 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 Key Pair Generation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Key Pair Generation FMT_MSA.3/Signer
FDP_ACF.1/Signer Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Maintenance FMT_MSA.3/Signer

Requirement	Dependencies	Fulfilled by
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

Requirement	Dependencies	Fulfilled by
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/SSA	FIA_UAU.1	FIA_UAU.2
FIA_AFL.1/User Manager	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	No dependents
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5/Signer	None	No dependents
FIA_UAU.5/Privileged User	None	No dependents
FIA_UID.2	None	No dependents

Requirement	Dependencies	Fulfilled by
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	No dependents
FMT_SMR.2	FIA_UID.1	FIA_UID.2
FPT_PHP.1	None	No dependents
FPT_PHP.3	None	No dependents

Requirement	Dependencies	Fulfilled by
FPT_RPL.1	None	No dependents
FPT_STM.1	None	No dependents
FPT_TDC.1	None	No dependents
FTP_TRP.1/SSA	None	No dependents
FTP_TRP.1/SIC	None	No dependents
FTP_ITC.1/CM	None	No dependents

6.7 Security Assurance Requirements

The security assurance requirement level is EAL 4 augmented with AVA_VAN.5. The assurance components are identified in the table below with the augmented item in bold.

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

Table 6-11 Security Assurance Requirements: EAL 4 augmented with AVA_VAN.5

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specifications
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and

Assurance Class	Assurance components
	automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5 Advanced methodical vulnerability analysis**

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

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

EAL 4 is therefore augmented with AVA_VAN.5.

7 TOE Summary Specification

To fulfil the Security Functional Requirements, the TOE comprises the following Security Functions (TSF): -

1. User Roles and Authentication (TSF_AUTH);
2. Key Security (TSF_CRYPTO);
3. Access and information flow control (TSF_CTRL);
4. Data protection (TSF_DP);
5. Audit (TSF_AUDIT); and
6. Communication protection (TSF_COMM).

Each of the TOE security functions is described in the following sections in detail.

7.1 TOE Security Functions

7.1.1 User Roles & Authentication (TSF_AUTH)

#FMT_SMR.2 Restrictions on security roles

The TOE maintains Privileged User (User Manager or Authenticated Application) and associates users with roles. The TOE identifies users by means of a unique user identifier. The TOE ensures that each user has only one role, consequently a Signer can't be a Privileged User. These users are stored and maintained in different subsystems and identified with different IDs. Privileged users are stored in the SAM database with unique identifiers whereas signer users are stored in the SSA database with their own unique identifiers.

The integrity of the records stored is protected by sequenced HMAC.

#FIA_UID.2 User identification before any action
#FIA_UAU.2 User authentication before any action
#FIA_UAU.5/Signer Multiple authentication mechanisms
#FIA_UAU.5/Privileged User Multiple authentication mechanisms

Privileged Users authenticate via client credentials to the TOE. The Privileged User authenticates himself with his user name and password using OAuth2 token.

Supported IdP will provide the assertion after successful authentication of the user and that assertion is added in the generated SAD at the time of authorisation.

#FIA_AFL.1 Authentication failure handling
#FIA_AFL.1/User Manager#FIA_AFL.1/SSA
The TOE handles authentication failures in a separate way for each role.

Privileged User (User Manager): Operator provides his credentials to connect with TOE and upon a TOE maintenance configurable number of unsuccessful attempts (default is 5) it is marked inactive.

Privileged User (Authenticated Application): After a TOE maintenance configurable number of unsuccessful (e.g. using wrong client credentials) authentication attempts (default is 5) the authenticated application is marked as inactive.

#FIA_ATD.1 User attribute definition
#FIA_USB.1 User-subject binding
#FMT_MSA.2
The TOE maintains accounts (with different security attributes) belonging to individual users. TOE validates the values assigned for these attributes.

7.1.2 Key Security (TSF_CRYPTO)

#FCS_CKM.1/RSA
#FCS_CKM.1/ECDSA
#FCS_CKM.1/AES
TOE calls certified CM to generate RSA, ECDSA and AES keys
#FCS_CKM.4
#FCS_COP.1/DIG_SIG_GEN
#FCS_COP.1/DIG_SIG_VER
#FCS_COP.1/HASH
#FCS_COP.1/HMAC
#FCS_COP.1/ENC
TOE performs the signature generation, verification, hashing, sequenced HMAC and encryption using the Certified CM.
#FCS_RNG.1
The TOE calls with appropriate parameters a CM certified in conformance with EN 419 221-5 [7] for any key management or cryptographic operations, random number generation.

7.1.3 Access and information flow control (TSF_CTRL)

#FDP_ACC.1/Privileged User Creation
#FDP_ACF.1/Privileged User Creation
#FMT_MSA.1/Privileged User
#FMT_MSA.3/Privileged User
#FMT_SMF.1
During eTugra SAM setup & initialization phase a default User manager is available which can create multiple user managers with different roles and register / create authenticated applications to communicate with TOE.

The TOE does not allow creation of new users until the Privileged User has been authenticated as described in section 7.1.1.

#FDP_ACC.1/Signer Creation
#FDP_ACF.1/Signer Creation
#FMT_MSA.1/Signer
#FMT_MSA.3/Signer
#FMT_MSA.2
#FMT_SMF.1
The TOE guarantees that only an Authenticated Application as a Privileged User can initiate Signer Creation and Signer key pair generation on behalf of the Signer. A typical Signer registration process involves registering Signer details (name, email address, phone number) and generating remote signing key pair and digital certificate. The Signer visits a Business Application (SCA) web page and provides their registration details for the Business Application. The business application (SCA) triggers the signer registration process.

The Business Application receives the registration details from the Signer and creates a user registration request for SSA.

#FDP_ACC.1/Signer Key Pair Generation
#FDP_ACF.1/Signer Key Pair Generation
#FDP_IFC.1/Signer
#FDP_IFF.1/Signer
Once the Signer details are registered in the Authenticated Application (SSA), it generates the signing key pair for the Signer. The TOE does not use pre-generated keys. To generate a signing key pair for a registered Signer the SSA must be authenticated as described in section 7.1.1.

Once the signing key pair has been generated, the SAM transfers the R.SVD (the public key) to a CSR and gets it signed with the remote signing private key, i.e. self-signed. In response to signing key pair generation request, the SSA returns the CSR which the Business Application can send to an issuing CA to get a signing certificate. Once the Business Application has obtained the signing certificate from the issuing CA, the Signer registration process is considered complete.

The TOE guarantees that the Signer is the owner of the R.Signer object.

#FDP_ACC.1/Signer Maintenance
#FDP_ACF.1/Signer Maintenance
#FDP_ACC.1/Signer Key Pair Deletion

#FDP_ACF.1/Signer Key Pair Deletion

The Authenticated Application (SSA) can modify or delete the R.Signer's security attributes (i.e. R.Reference_Signer_Authentication_Data) only after its authorisation (as described in section 7.1.1).

#FDP_ACC.1/Supply DTBS/R
#FDP_ACF.1/Supply DTBS/R
To perform signature on a PDF document, the signature creation application computes the PDF document hash along with other attributes and sends it to the Authenticated Application (SSA) to sign this hash with the Signer's signing key which then forwards it to SAM for the signature computation after authorisation done from the signer user either from the SIC (e.g. mobile device) or after successful authentication from IdP, SSA creates a SAD which is then passed to SAM along with DTBS/R for key activation and signature operation.

#FDP_ACC.1/Signing
#FDP_ACF.1/Signing
The Signer has sole control over its remote signing keys by a dynamic authorization mechanism.

Once the SAM verifies the SAD and user IdP assertion/token it activates the signer key using the R.Authorisation_Data and performs the signature operation and returns the signature back to SSA which then forwards it to SCA for the PDF signing operation completion.

The TOE ensures that Signer shall authorise any subsequent use of the signing key.

#FDP_ACC.1/TOE Maintenance
#FDP_ACF.1/TOE Maintenance
#FMT_MTD.1
#FMT_SMF.1
#FDP_IFC.1/Privileged user
#FDP_IFF.1/Privileged user
Only authorised authenticated User manager of particular role (Administrator and Security Officer) can maintain the TOE configuration data via Administration APIs. The authentication of Privileged Users is described in section 7.1.1.

#FDP_ETC.2/Signer
#FDP_ITC.2/Signer
#FDP_ETC.2/Privileged user
#FDP_ITC.2/Privileged user
Data is only imported/exported by the TOE after successful authentication of the expected user as defined by the relevant SFP (authentication performed as described in section 7.1.1). The communication channel is protected and integrity ensured as described in section 7.1.6.

7.1.4 Data protection (TSF_DP)

#FPT_PHP.1 Passive detection of physical attack

The TOE implements security functionality to detect physical tamper. If the hardware sensors detect tamper the tamper detection switch of the HSM is triggered, which erases the HSM keys.

#FPT_PHP.3 Resistance to physical attack

The TOE detects when the enclosure of the TOE is opened and zeroises sensitive data, and terminates main power. This ensures that the integrity and confidentiality of the assets are preserved. During tamper state, all functionality of the TOE is stopped and no service is provided (both signatory ones and administrative ones) even if the TOE is hardware restarted. When the TOE is hardware restarted it will maintain the tamper state such that the previous tamper condition can be reported.

#FPT_RPL.1 Replay detection

The TOE rejects the signature operation if a SAD is being used more than once. The communication between SSA and Signer are based on a proprietary SAP. The SAP is protected against replay, bypass and forgery attack, using a salt (random value to avoid replay attack), a validity period and the PKCS#1 authorization signature of the Signer.

#FPT_STM.1 Reliable time stamps

TOE gets the time source using Fortigate, it gets authenticated via Active Directory and gets the authentication token. TOE connects with the Fortigate on a particular port through certificate-based authentication. If authentication is successful, the communication is done via a secure channel. Fortigate communicates with multiple NTP Servers, picks the most accurate time and provides it to TOE.

#FPT_TDC.1 Inter-TSF basic TSF data consistency

Whenever the TOE exchanges sensitive data with other components outside of the TOE boundary uses data integrity either on the data or on the communication channel when interpreting the data. The TOE guarantees that the interpretation of main resources will remain consistent. However, some of the main resources of the TOE are stored outside of the TOE. These resources are handled appropriately concerning integrity and confidentiality. Integrity is ensured through secure symmetric key

7.1.5 Audit (TSF_AUDIT)

#FAU_GEN.1 Audit Generation
#FAU_GEN.2 User identity association

The TOE uses an audit Database outside the TOE boundaries. The TOE logs every security related event. Each audit record contains date and time of the event (using reliable timestamp), type of event, subject identity (the identity of the user that caused the event if applicable, i.e., an identified user initiated the event), and the outcome (success or failure) of the event. The audit trail does not include any data which allows the retrieval of sensitive data.

The integrity of audit log is ensured through digital signature applied to it.

7.1.6 Communication protection (TSF_COMM)

#FDP_UCT.1 Basic data exchange confidentiality
#FDP_UIT.1 Data exchange integrity
#FTP_TRP.1/SSA FTP_TRP.1/SIC Trusted path
#FTP_ITC.1/CM Inter-TSF trusted channel
The TOE provides protection of user data while in transit. It ensures both confidentiality and integrity. The SIC securely communicates with the SSA, the SCA with the SSA and the SSA with the TOE over TLS v1.2/1.3 channel. Communication with the CM is through a secure channel

7.2 Fulfilment of the SFRs

This section shows that the TSFs are appropriate to fulfil the TOE Security Functional Requirements as specified in chapter 6.3.

The mapping of SFRs and TSFs is given in Table 7-1.

Table 7-1 SFR – TSF relationship

SFR	TSF
FAU_GEN.1	TSF_AUDIT
FAU_GEN.2	TSF_AUDIT
FCS_CKM.1/*	TSF_CRYPTO
FCS_CKM.4	TSF_CRYPTO
FCS_COP.1/*	TSF_CRYPTO
FCS_RNG.1	TSF_CRYPTO
FDP_ACC.1/Privileged User Creation	TSF_CTRL
FDP_ACF.1/Privileged User Creation	TSF_CTRL
FDP_ACC.1/Signer Creation	TSF_CTRL
FDP_ACF.1/Signer Creation	TSF_CTRL

SFR	TSF
FDP_ACC.1/Signer Key Pair Generation	TSF_CTRL
FDP_ACF.1/Signer Key Pair Generation	TSF_CTRL
FDP_ACC.1/Signer Maintenance	TSF_CTRL
FDP_ACF.1/Signer Maintenance	TSF_CTRL
FDP_ACC.1/Signer Key Pair Deletion	TSF_CTRL
FDP_ACF.1/Signer Key Pair Deletion	TSF_CTRL
FDP_ACC.1/Supply DTBS/R	TSF_CTRL
FDP_ACF.1/Supply DTBS/R	TSF_CTRL
FDP_ACC.1/Signing	TSF_CTRL
FDP_ACF.1/Signing	TSF_CTRL
FDP_ACC.1/TOE Maintenance	TSF_CTRL
FDP_ACF.1/TOE Maintenance	TSF_CTRL
FDP_ETC.2/Signer	TSF_CTRL
FDP_IFC.1/Signer	TSF_CTRL
FDP_IFF.1/Signer	TSF_CTRL
FDP_ETC.2/Privileged User	TSF_CTRL
FDP_IFC.1/Privileged user	TSF_CTRL
FDP_IFF.1/Privileged User	TSF_CTRL
FDP_ITC.2/Signer	TSF_CTRL
FDP_ITC.2/Privileged User	TSF_CTRL
FDP_UCT.1	TSF_COMM
FDP_UIT.1	TSF_COMM
FIA_AFL.1/*	TSF_AUTH
FIA_ATD.1	TSF_AUTH
FIA_UAU.2	TSF_AUTH
FIA_UAU.5/Signer	TSF_AUTH

SFR	TSF
FIA_UAU.5/Privileged User	TSF_AUTH
FIA_UID.2	TSF_AUTH
FIA_USB.1	TSF_AUTH
FMT_MSA.1/Signer	TSF_CTRL
FMT_MSA.1/Privileged User	TSF_CTRL
FMT_MSA.2	TSF_AUTH, TSF_CTRL
FMT_MSA.3/Signer	TSF_CTRL
FMT_MSA.3/Privileged User	TSF_CTRL
FMT_MTD.1	TSF_CTRL
FMT_SMF.1	TSF_CTRL
FMT_SMR.2	TSF_AUTH
FPT_PHP.1	TSF_DP
FPT_PHP.3	TSF_DP
FPT_RPL.1	TSF_DP
FPT_STM.1	TSF_DP
FPT_TDC.1	TSF_DP
FPT_TRP.1/SSA	TSF_COMM
FPT_TRP.1/SIC	TSF_COMM
FTP_ITC.1/CM	TSF_COMM

7.2.1 Security Requirements Coverage

Each TOE Security Functional Requirement is implemented by at least one Security Function (see Table 7-1).

8 Glossary and Acronyms

8.1 Acronyms

AC	Access Control
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
CM	Cryptography Module certified according to EN 419221-5:2018
CSR	Certificate Signing Request
Certificate	Certificate for electronic signature as defined in eIDAS article 3.
DTBS/R	Data To Be Signed Representation
EAL	Evaluation Assurance Level
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
RDBMS	Relational database management system
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SIC	Signer’s Interaction Component

SSA	Server Signing Application
SVD	Signature Verification Data
ST	Security Target
TOE	Target of Evaluation
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
QSCD	Qualified Electronic Signature (or Electronic Seal) Creation Device as defined in the eIDAS Regulation [8]

9 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

[5] EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, Feb 2019

[6] EN 419241-1:2018, Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements

[7] EN 419221-5:2018, Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services

[8] 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

[9] ETSI TS 119 312 v1.4.1 (2021-08) Electronic Signature and Infrastructures (ESI); Cryptographic Suites

[10] SOG-IS, Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, version 1.3, February 2023

[11] ETSI EN 319 411-1 v1.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[12] ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastuctures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[13] COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[14] 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.

[15] RSA Laboratories, PKCS #1: RSA Encryption Standard, Version v2.2, October 27, 2012

[16] FIPS PUB 186-5, Federal Information Processing Standards Publication, Digital Signature Standard (DSS), February 3, 2023

[17] FIPS PUB 140-3, Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, March 22, 2019

[18] X9.62-1998, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), September 20, 1998

[19] RFC 6151 – Updated Security Considerations for the MD5 Message-Digest and teh HMAC-MD5 Algorithms, March 2011

[20] BSI AIS 20 / AIS 31, Functionality classes for random number generators Version 2.0, 18 September 2011

[21] NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

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

[23] FIPS 202 Federal Information Processing Standards Publication 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015

[24] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[25] AGD_OPE – Operational User Guidance v9, January 2024

[26] AGD_PRE – Preparation Procedure v8, January 2024

[27] Certification Report - Thales Luna K7 Cryptographic Module v1, July 2022

[28] Security Target - Thales Luna K7 Cryptographic Module Rev. M, May 2022