CEN/TC 224

Date: 2018-05-11

419 241-2

CEN/TC 224

Secretariat: AFNOR

Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing

ICS:

Descriptors:

Contents

List of Tables

List of Figures

Foreword

This document (prEN 419 241-2:2017) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is a working document.

Revision History

PRE-RELEASE HISTORY FOR EDITORIAL TRACKING ONLY, REPLACE FOR FINAL PP

v0.01	2015-08-28	Initial draft for TC224 WG17 group discussion containing overview, conformance claim, assets and threats
v0.02	2015-11-10	Updated assets and threats based on discussions at the TC224 WG17 meeting in La Ciotat September, 2015 as well as received comments following the meeting.
v0.03	2015-11-25	Updated based on comments from BSI and Thales prior CEN TC244 WG17 meeting in Kochel, November 2015.
v0.4	2016-02-08	Updated based on comments to v0.03.
v0.5	2016-03-08	Updated with SFRs.
v0.6	2016-06-05	Updated with Security requirements and comments for v0.5
v0.7	2016-08-08	Updated with SFRs comments to version 0.6. Usage description updated, Subjects simplified. SFRs heavily restructured to handle comments.
v0.8	2016-11-11	Updated based on comments to v0.7.
v0.9	2016-11-20	Updated based on comments to v0.8. Rationale completed.
v0.10	2016-12-16	Updated based on comments to v0.9 received by CEN TC224 WG17. In particular for direct and indirect authentication.
v0.11	2017-01-27	Updated based on comments to v0.10 received by CEN TC224 WG17 and Oppida.
v0.12	2017-02-02	Updated based on comments to v0.11 received by CEN TC224 WG17 and Oppida primary during the London Meeting.
v0.13	2017-09-05	Updated based on comments to v0.12 received from the evaluator from Oppida.
v0.14	2017-09-26	Updated based on comments received by CEN TC224 WG17 during Paris meeting.
v0.15	2017-10-19	Updated based on comments received by CEN TC224 WG17 during GotoMeeting 2017-10-19.
v0.16	2018-05-11	Updated based on comments received by BSI as part of SOG-IS review.

[**Put correct date for released version]

Introduction

This Protection Profile for ‘QSCD for Server Signing’ (SAM-PP) is issued by the European Committee for Standardization (CEN) TC 224.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 3.1r4 [CC1], [CC2] and [ICC3].

This document is part of the EN 419 241 series that consists of the following parts:

- EN 419 241-1: Security Requirements for Trustworthy Systems Supporting Server Signing;
- EN 419 241-2: This document

Further details of this series can be found in EN 419 241-1.

Document Structure

Section 1 provides the introductory material for the Protection Profile.

Section 2 describes terms and definitions

Section 3 contains the introduction

Section 3.3.6 provides the conformance claim

Section 5 provides the Security Problem Definition. It presents the Assets, Threats, Organisational Security Policies and Assumptions related to the TOE.

Section 6 defines the security objectives for both the TOE and the TOE environment.

Section 7 contains an extended component definition to include random number generation

Section 8 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [CC2] and Part 3 [CC3] that must be satisfied by the TOE.

Section 9 provides rationales to demonstrate that:

- Security Objectives satisfy the policies and threats
- SFR match the security Objectives
- SFR dependencies are satisfied
- The SARs are appropriate.

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Scope

This part of EN 419 241 specifies a protection profile for a Signature Activation Module (SAM), which is aimed to meet the requirements of a QSCD as specified in Regulation (EU) No 910/2014 [eIDAS].

2 Terms and definitions

For the purposes of this document, the symbols, abbreviations, terms and definitions given in [EN 419 241-1], [EN 419 221-5] and [eIDAS] article 3 apply.

Common Criteria terms and definitions are given in [CC1].

Additional terms defined or precisions for the purposes of this document are listed below.

CA	Certification Authority
CM	Cryptographic Module certified according to [EN 419 221-5]
CSR	Certification Signing Request
Certificate	Certificate for electronic signature as defined in [eIDAS] article 3.
Delegated Party	Subcontractor of the TSP or notified eID provider according to eIDAS regulation used for authentication.
Digital Signature Value	The result of a cryptographic operation involving the signing key. Within this document, Seal, Signature, Digital Signature or Digital Seal denote Digital Signature Value.
DTBS/R(s)	One or a set of DTBS/R.
One-time signing key	A signing key created, used and disposed based on one a single authorization, typically linked to a single session signing DTBS/R(s). Contrary to signing keys, which may be used in several signing sessions.

3 Introduction

This section provides document management and overview information that is required to carry out protection profile registration. Section 1.1 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. Section 1.3 "TOE Overview" summarises the TOE in a narrative form. As such, these sections give an overview to the potential user to decide whether the PP is of interest. It is usable as a standalone abstract in PP catalogues and registers.

3.1 Protection Profile Reference

Title	Common Criteria Protection Profile – Protection Profile for QSCD for Server Signing
CC revision	v3.1 release 4
PP version	0.16
Authors	WG17
Keywords	Server Signing

3.2 Protection Profile Overview

3.2.1 European Legislation

The Regulation (EU) No 910/2014 [eIDAS] recital 52 considers the creation of remote electronic signatures, where the electronic signature creation data is managed remotely by a trust service provider on behalf of the signatory.

Such trust service providers should apply specific management and administrative security procedures in order to guarantee that the electronic signature creation environment is reliable and used under the sole control of the signatory.

This regulation requires, for qualified electronic signatures, the use of qualified electronic signature creation devices and for qualified electronic seals, the use of qualified electronic seal creation devices, as defined in the regulation. In the present document, both types of devices are referred to as QSCD.

3.3 TOE Overview

A trustworthy system supporting server signing (TW4S) is a system that offers remote digital signatures as a service. It ensures that signer’s signing key or keys are only used under the sole control of the signer for the intended purpose.

In this document, the TW4S uses a Cryptographic Module to generate the signing key and create the digital signature value.

The system consists of a local and remote environment. The signer is in the local environment and interacts using a device (e.g. laptop, tablet or smart phone) with the Server Signing Application (SSA) in the remote environment.

The purpose of the interaction between the device and SSA is for the signer to utilize the SSAs signing service. The signature operation is performed using a Signature Activation Protocol (SAP), which requires that Signature Activation Data (SAD) be provided at the local environment. The SAD binds together three elements: signer authentication with the signing key and the data to be signed (DTBS/R(s)).

To ensure the signer has sole control of his signing keys, the signature operation needs to be authorised. This is carried out by a Signature Activation Module (SAM), which can handle one endpoint of SAP, verify SAD and activate the signing key within a Cryptographic Module. Both the Cryptographic Module and the SAM are to be located within a tamper protected environment. SAD

verification means that the SAM checks the binding between the three SAD elements as well as checking that the signer is authenticated.

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

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

In case the signer authentication is not performed directly by the SAM, the SAM has to assume (on the environment) that part of or complete authentication has taken place and rely on an assertion. In this PP signer authentication means that the signer has been authenticated in one of the three ways mentioned above.

The SAM module is the TOE of this PP. The TOE and Cryptographic Module certified against [EN 419 221-5] is required to obtain a QSCD.

The illustration below gives an overview of the environment on which the TOE is placed.

The signer is located in the local environment with a user interface on device (e.g. laptop, tablet, smartphone). The user interface can display documents for the signer. The device uses a signer interaction component (SIC) to communicate with the SSA. The SSA forwards the communication from the SIC or from the SSA to the QSCD. Inside the QSCD the SAM receives the messages and optionally communicates with the SSA to obtain relevant data. When the SAM module has verified SAD, it can authorise the activation of the signing key within the Cryptographic Module and produce a digital signature value. The value is returned to the SSA and may be further delivered to the SCA or SIC. From a TOE point of view the SSA and User Interface acts as supporting modules which displays document and forwards communication messages.

The TOE generates audit records for all security related events and relies on the SSA to store and provide access control for the records.

The TW4S relies on other services:

- Signers must be identified and registered. It may involve establishment of authentication mechanism for a signer.
- Signing keys are certified by a Certification Authority.
- The Signature Creation Application is responsible for creating the signed document using the signature values provided by the TW4S.

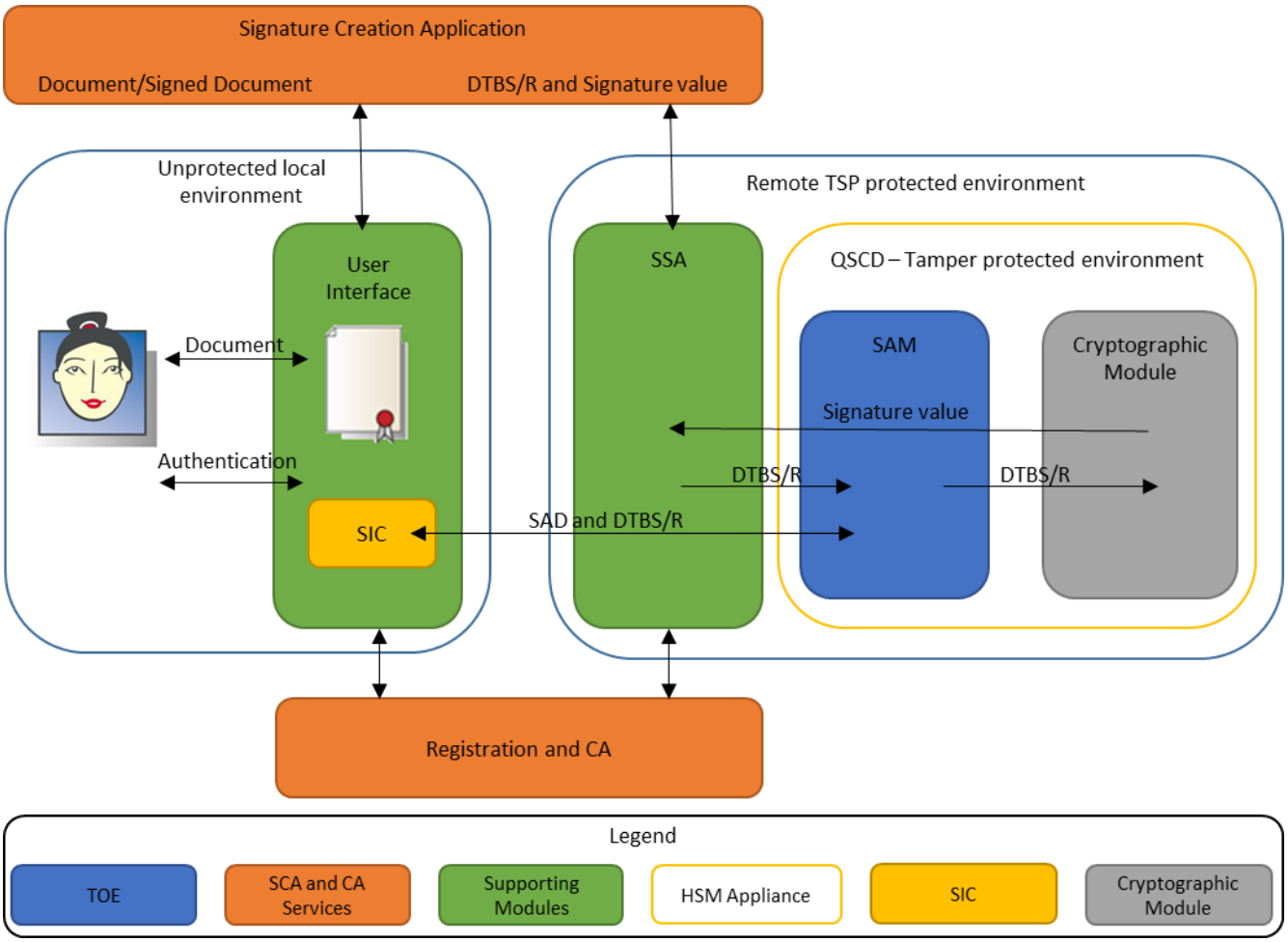


Figure 1

3.3.1 TOE type

The TOE is a software component, which implements the Signature Activation Protocol (SAP). It is either deployed within the tamper protected part of the Cryptographic Module or alternatively in a dedicated tamper protected environment, that is connected to the Cryptographic Module via a trusted channel.

It uses the Signature Activation Data (SAD) from the signer to activate the corresponding signing key for use in a Cryptographic Module.

Together the TOE and Cryptographic Module are a QSCD.

3.3.2 TOE life cycle

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

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

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

Installation and configuration: The TSP installs and configures the TOE with the appropriate configuration and initialisation data. Installation may allow creating the Privileged Users.

Operational phase: In operation, the TOE can be used by Privileged Users to create Privileged Users and Signers. Privileged Users can maintain TOE configuration. Privileged Users and Signers may

generate signature keys for a Signer. Privileged Users and Signers can supply the data to be signed to the TOE, but only Signer can authorise a signature creation.

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

3.3.3 Usage and major security features of the TOE

The major security features of the TOE are:

- Operator management:
  - Privileged Users can create other Privileged Users.
- System management
  - Privileged Users can handle system configuration.
- Signer management covers:
  - Privileged Users can create Signers
  - Privileged Users can assign on of the three authentication schemes (direct, indirect or mixed) to a Signer.
  - Privileged Users or Signers can generate signing keys and signature Verification Data (SVD) using a Cryptographic Module and assign the signing key identifier and SVD to a Signer.
  - Privileged Users or Signers can disable a signing key identifier to be used by a Signer.
- Signature operation
  - Privileged Users or Signers can supply a DTBS/R(s) to be signed.
  - The link between signer authentication, DTBS/R(s) and signing key identifier is handled by the Signature Activation Data (SAD). This SAD is securely exchanged with the TOE using the Signature Activation Protocol (SAP). Within the TOE the following actions are performed:
    - The SAD is verified in integrity.
    - The SAD is verified that it binds together the Signer authentication, a DTBS/R(s) and signing key identifier.
    - The Signer identified in the SAD is authenticated using one of the three authentication schemes.
    - The DTBS/R(s) used for signature operations is bound to the SAD.
    - The signing key identifier is assigned to the Signer.
    - The TOE uses Authorisation Data to activate the signing key within the Cryptographic Module.
    - The TOE uses the Cryptographic Module to create signatures.
- The TOE generates audit records for all security related events and relies on the SSA to store and provide access control for the records.

The TOE handles data assets as specified in 5.1.

3.3.4 TOE Environment general overview

This PP is aimed to support TSPs requiring to use a QSCD for server signing.

The TOE is expected to:

1. operate as parts of server signing system as specified in [EN 419 241-1]
2. be used by a TSP applying security policies as required by TSPs providing signature creation services
3. used in conjunction with TSPs issuing certificates

3.3.5 Available non-TOE hardware/software/firmware

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

- A Signature Creation Application (SCA) that manages the document to be signed and transfers that to the SSA, either directly or through the SIC.
- A SSA component that handles communications between SAM in the QSCD and SIC in the signer device.
- A SIC used locally by the signer to communicate with the remote systems.
- A Cryptographic Module certified against [EN 419 221-5], which supports the operation of the TOE.

3.3.6 Options

The Protection Profile includes options, which the ST writer shall specify. To assist the ST writer identifying these options, they are summarised in the following table:

Option	Description
Deployment	The TOE may be deployed in a Cryptographic Module or in a dedicated hardware module. The ST writer shall pay special attention to the SFRs FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RNG.1, FPT_PHP.1, FPT_PHP.3 and FTP_ITC.1/CM as these SFRs may be met differently depending on the deployment.

Table 1

4 Conformance Claim

4.1 CC Conformance Claim

This protection profile (PP) claims to be Common Criteria Part 2 extended and Common Criteria Part 3 conformant and written according to the Common Criteria version 3.1 R4 [CC1], [CC2] and [CC3].

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

- AVA_VAN.5 Advanced methodical vulnerability analysis

4.2 PP Claim

This PP does not claim conformance to any other Protection Profile.

4.3 Conformance Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

4.4 Conformance Statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

5 Security Problem Definition

5.1 Assets

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

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

Application Note 1

The integrity and confidentiality of the signing key and the link between the R.Signing_Key_Id and the signing key is the responsibility of the Cryptographic Module. The TOE shall ensure that only the signer can use the signing key under his sole control.

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

Application Note 2

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

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

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

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

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

Application Note 3

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

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

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

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

Application Note 4

If the SAD does not require encrypted data then the confidentiality requirement is considered fulfilled. The ST writer shall describe which part of the SAD shall be protected in confidentiality.

Application Note 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 6

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

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

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

The ST writer shall describe what R.Signing_Key_Id is for a specific TOE.

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

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

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

Application Note 7

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

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

Application Note 9

If the R.Signer does not require encrypted data then the confidentiality requirement is considered fulfilled. The ST writer shall describe which part of the R.Signer shall be protected in confidentiality.

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

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

Application Note 10

The R.Reference_Signer_Authentication_Data is used by the TOE to authenticate the signer, and the R.Authorisation_Data is used by the TOE to activate a signing key in the Cryptographic Module.

Application Note 11

If the R.Reference_Signer_Authentication_Data does not require encrypted data then the confidentiality requirement is considered fulfilled. The ST writer shall describe which part of the R.Reference_Signer_Authentication_Data shall be protected in confidentiality.

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

Application Note 12

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

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

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

Application Note 13

If the R.Reference_Privileged_User_Authentication_Data does not require encrypted data then the confidentiality requirement is considered fulfilled. The ST writer shall describe which part of the R.Reference_Privileged_User_Authentication_Data shall be protected in 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.

5.2 Subjects

This following list of subjects interact with the TOE.

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

Application Note 14

The list of subjects described in [EN 419 241-1] clause 6.2.1.2 SRG M.1.2 contains more roles as it covers the whole T4WS.
The ST writer shall describe the specific roles it implements and how these relate to authorisation rules in the SFRs.

Application Note 15

The SSA plays a special role as it interacts directly with the TOE. Privileged Users can interact with the TOE directly or via the SSA. If the SSA as a service can perform administrative functions, e.g. creating signer, this is in this PP considered as Privileged User.

Application Note 16

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].

5.3 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.

5.3.1 Enrolment

The threats during enrolment are:

T.ENROLMENT_SIGNER_IMPERSONATION

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

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

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

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

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

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

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

The asset R.Reference_Signer_Authentication_Data is threatened.

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

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

T.SVD_FORGERY

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

The asset R.SVD is threatened.

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

Application Note 17

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

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

5.3.2 Signer Management

T.ADMIN_IMPERSONATION

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

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

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

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

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

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

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

5.3.3 Usage

This section describes threats for signature operation including authentication.

T.AUTHENTICATION_SIGNER_IMPERSONATION

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

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

T.SIGNER_AUTHENTICATION_DATA_MODIFIED

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

The asset R.Reference_Signer_Authentification_Data is threatened.

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

T.SAP_BYPASS

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

The asset R.SAD is threatened.

T.SAP_REPLAY

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

The asset R.SAD is threatened.

T.SAD_FORGERY

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

The asset R.SAD is threatened.

T.SIGNATURE_REQUEST_DISCLOSURE

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

The assets R.DTBS/R and R.SAD are threatened.

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

T.DTBSR_FORGERY

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

The asset R.DTBS/R is threatened.

T.SIGNATURE_FORGERY

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

The asset R.Signature is threatened.

Application Note 18

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

5.3.4 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 19

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

T. AUTHORISATION_DATA _DISCLOSE

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

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

T.CONTEXT_ALTERATION

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

5.4 Relation between threats and assets

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

Asset	Security Dimensions	Threats
R.Signing_Key_Id	Integrity	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Authorisation_Data	Integrity	T.AUTHORISATION_DATA_UPDATE
	Confidentiality	T.AUTHORISATION_DATA_UPDATE T.AUTHORISATION_DATA_DISCLOSE
R.SVD	Integrity	T.SVD_FORGERY T.ADMIN_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
R.DTBS/R	Integrity	T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY
	Origin authentication	T.DTBSR_FORGERY
R.SAD	Integrity	T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION T.SAP_BYPASS T.SAP_REPLAY T.SAD_FORGERY
	Confidentiality	T.AUTHENTICATION_SIGNER_IMPERSONATION T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrity	T.SIGNATURE_FORGERY
R.Audit	Integrity	T.AUDIT_ALTERATION
R.Signer	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION
R.Reference_Signer_Authentication_Data	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T. SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Confidentiality	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE

Asset	Security Dimensions	Threats
		T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Privileged_User	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.Reference_Privileged_User_Authentication_Data	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
	Confidentiality	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.RANDOM	Integrity	T.RANDOM
	Confidentiality	T.RANDOM
R.TSF_DATA	Integrity	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

Table 2

5.5 Organisational Security Policies

The 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 20

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

5.6 Assumptions

A.PRIVILEGED_USER

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

A.SIGNER_ENROLMENT

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

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

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

A.SIGNER_DEVICE

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

A.CA

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

A.ACCESS_PROTECTED

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

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

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

Application Note 21

The ST writer shall describe which data is managed outside the TOE.

A.AUTH_DATA

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

A.TSP_AUDITED

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

A.SEC_REQ

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

6 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.

6.1 Security objectives for the TOE

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

6.1.1 Enrolment

OT.SIGNER_PROTECTION

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

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

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

OT.SIGNER_KEY_PAIR_GENERATION

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

OT.SVD

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

6.1.2 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 22

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

OT.PRIVILEGED_USER_PROTECTION

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

OT.SIGNER_MANAGEMENT

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

6.1.3 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 23

Where the TOE derives authorisation data from authentication data in the SAD and uses this to activate the signing key in the cryptographic module this function can depend on the controls provided by the cryptographic module.

Application Note 24

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

OT.SAP

The TOE shall implement the server-side endpoint of a Signature Activation Protocol (SAP), which provides the following:

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

Application Note 25

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

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

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION

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

OT.DTBSR_INTEGRITY

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

OT.SIGNATURE_INTEGRITY

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

OT.CRYPTO

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

6.1.4 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.

6.2 Security Objectives for the Operational Environment

OE.SVD_AUTHENTICITY

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

OE.CA_REQUEST_CERTIFICATE

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

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

OE.CERTIFICATE_VERFICATION

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

OE.SIGNER_AUTHENTICATION_DATA

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

OE.DELEGATED_AUTHENTICATION

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

In addition, the TSP shall ensure that:

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

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

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

OE.DEVICE

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

OE.ENV

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

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

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

OE.CRYPTOMODULE_CERTIFIED

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

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

Application Note 26

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

OE.TW4S_CONFORMANT

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

6.3 Security Problem Definition and Security Objectives

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

TOE Security Objectives and threats.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD
Enrolment					
T.ENROLMENT_SIGNER_IMPERSONATION		X	X		
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		X	X		
T.SVD_FORGERY				X	X
Signer Management					
T.ADMIN_IMPERSONATION					
T.MAINTENANCE_AUTHENTICATION_DISCLOSE			X		
Usage					
T.AUTHENTICATION_SIGNER_IMPERSONATION					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X		
T.SAP_BYPASS					
T.SAP_REPLAY					
T.SAD_FORGERY					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
System					
T.AUTHORISATION_DATA_UPDATE					
T.AUTHORISATION_DATA_DISCLOSE					
T.CONTEXT_ALTERATION					
T.AUDIT_ALTERATION					
T.RANDOM					

Table 3

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

Table 4

	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO
Enrolment							
T.ENROLMENT_SIGNER_IMPERSONATION							
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED							
T.SVD_FORGERY							X
Signer Management							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Usage							
T.AUTHENTICATION_SIGNER_IMPERSONATION		X					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X	X			
T.SAP_BYPASS			X				
T.SAP_REPLAY			X				
T.SAD_FORGERY			X	X			
T.SIGNATURE_REQUEST_DISCLOSURE			X				
T.DTBSR_FORGERY					X		
T.SIGNATURE_FORGERY						X	X
System							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Table 5

TOE Security Objectives and Organizational Security Policies.

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

Table 6

Threats and Security Objectives for the environment.

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

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
T.SAD_FORGERY			X	X			
T.DTBSR_FORGERY				X			
T.SIGNATURE_FORGERY							
System							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Table 7

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

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Organisational Security Policies							
OSP.TSP_AUDITED							X
OSP.RANDOM							
OSP.CRYPTO						X	
Assumptions							
A.PRIVILEGED_USER							X

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
A.SIGNER_ENROLMENT					X		
A.SIGNER_AUTHENTICATION_DATA_PROTECTION			X				
A.SIGNATURE_REQUEST_DISCLOSURE				X			
A.SIGNER_DEVICE				X			
A.CA		X					
A.ACCESS_PROTECTED					X		
A.AUTH_DATA				X			
A.TSP_AUDITED					X		
A.SEC_REQ							X

Table 8

6.4 Rationale for the security objectives

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

6.4.1 Threats and objectives

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

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

It is also covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring the TOE to be able to assign signer authentication data to the signer.

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

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

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

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

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

T.SVD_FORGERY is covered by OT.SIGNER_KEY_PAIR_GENERATION requiring a Cryptographic Module to generate signer key pair.

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

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

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

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

T.ADMIN_IMPERSONATION is covered by OT.SIGNER_MANAGEMENT and OT.PRIVILEGED_USER_AUTHENTICATION requiring any changes to the signer representation and attributes are carried out in an 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 must completed.

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

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

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

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

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

It is also covered by OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION requiring signature authentication data to be protected during transmit to the TOE.

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

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

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

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

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

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

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

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

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

T.AUTHORISATION_DATA_UPDATE is covered by OT.SYSTEM_PROTECTION requiring any 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.

6.4.2 Organizational security policies and objectives

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

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

6.4.3 Assumptions and 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] where clause SRG_M.1.8 requires that administrators are trained.

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

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

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

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

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

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

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

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

7 Extended Components Definitions

7.1 Class FCS: Cryptographic Support

The Class FCS: Cryptographic Support as defined in [CC2] is extended with a new family: Generation of Random Numbers (FCS_RNG). The family is concerned with generation of random numbers. The following picture illustrates the decomposition of the Class FCS: Cryptographic Support with the added family FCS_RNG:

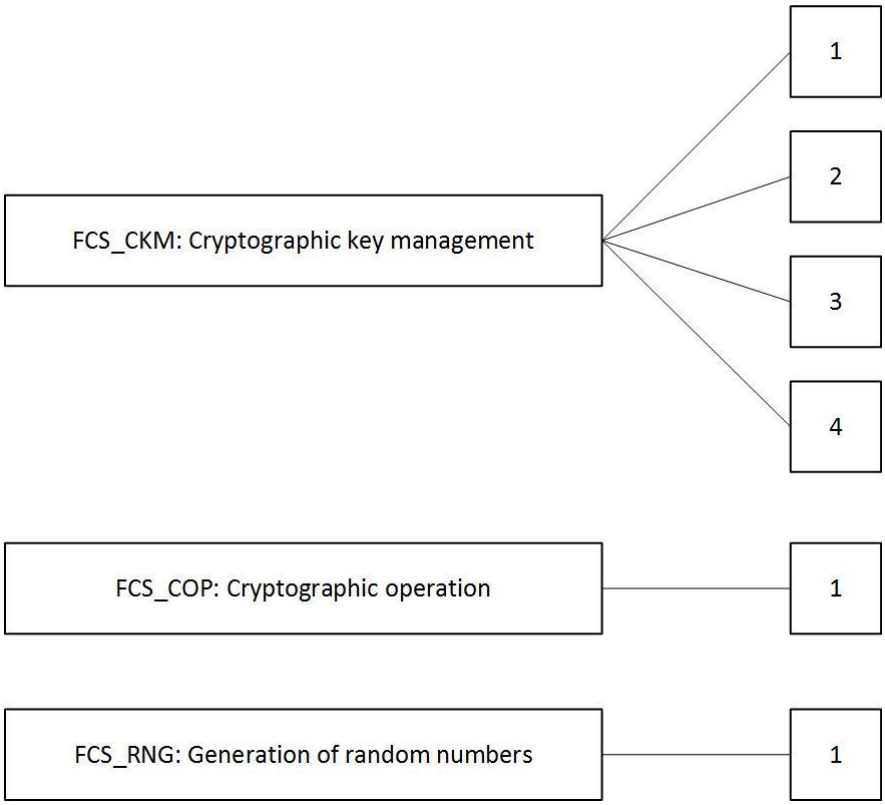


Figure 2

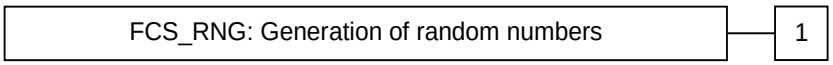
7.1.1 Generation of Random Numbers (FCS_RNG)

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

Family behaviour:

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

Component levelling:



Management: FCS_RNG.1

There are no foreseen management activities.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Generation of random numbers

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

FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

Application Note 27

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.

8 Security Requirements

8.1 Typographical Conventions

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

- Refinements made in the PP are always updates of the text for the SFR. They are marked in bold and the original text is indicated in a footnote.
- Selections made in this PP are written in italics, and the original text is indicated in a footnote. Selections that are left to be filled in by the Security Target author appear in square brackets with an indication that a selection is to be made, [selection:], and the description of selections options are written in italics.
- Assignments made in this PP are written in italics, and the original text is indicated in a footnote. Assignments that are left to be filled in by the Security Target author appear in square brackets with an indication that an assignment is to be made, [assignment:], and the assignment description is written in italics.
- Iterations are denoted by a slash "/" and the iteration indicator after the component identifier.

8.2 Subjects, Objects and Operations

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

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

Table 9

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.Signaer signature key pair
R.Signature	The result of a signature operation
R.TSF_DATA	TOE Configuration Data

Table 10

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

Table 11

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

Create Signer

- FDP_ACC.1/Signer Creation using FDP_ACF.1/Signer Creation describes access control requirements for creating 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 describes rules for how signing key pair are generated

Signer Key Pair Deletion

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

Signer Maintenance

- FDP_ACC.1/Signer Maintenance using FDP_ACF.1/Signer Maintenance describes access control requirements for updating the R.Reference_Signer_Authenticaton_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.

Privileged User object

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

Privileged User Creation

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

TOE Maintenace

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

Audit

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

Communication

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

8.4 Security Functional Requirements

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

8.4.1 Security Audit (FAU)

FAU_GEN.1 Audit Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and
c) Privileged User management;
d) Privileged User authentication;
e) Signer management;
f) Signer authentication;
g) Signing key generation;
h) Signing key destruction;
i) Signing key activation and usage including the hash of the DTBS/R(s); and R.Signature;
j) Change of TOE configuration;
k) [assignment: *other specifically defined auditable events*][1].

Application Note 28

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

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

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

Application Note 29

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

Application Note 30

Some implementations may not, for privacy reasons, record the R.DTBS/R in the audit log. For such systems, the ST writer shall describe how the log can be used to demonstrate that particular DTBS/R(s) was signed.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: *Type of action performed (success or failure), identity of the role which performs the operation.* [assignment: *other audit relevant information*]]**[2].

Application Note 31

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

FAU_GEN.2 User identity association

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

8.4.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 32

The TOE is expected to use a cryptographic module certified in conformance with [EN 419 221-5], see also OE.CRYPTOMODULE_CERTIFIED for key generation. Although the TSF may not generate keys itself, this SFR expresses the requirement for the TSF to invoke the cryptographic module with the appropriate parameters whenever key generation is required.

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

Application Note 33

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 34

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

Although the TSF may not destruct keys, this SFR expresses the requirement for the TSF to invoke the cryptographic module with the appropriate parameters whenever key destruction is required.

The Security Target must specify the method(s) of secure destruction of all secret keys and all support keys, and must ensure that all are covered by a secure destruction method. If necessary, then more

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

than one iteration of FCS_CKM.4 may be included to describe different standards for secure deletion. The 'list of standards' in the final assignment may be met in the Security Target by simply providing a description of the action taken to zeroise the keys rather than referencing an external standard.

Application Note 35

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

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 36

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

Application Note 37

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

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

FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1 The TSF shall provide a [selection: *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 38

For more information on the selections and assignments, see the SFR definition in section 7.1.1.

Application Note 39

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

8.4.3 User Data Protection (FDP)

FDP_ACC.1/Privileged User Creation	Subset access control

FDP_ACC.1.1/ Privileged User The TSF shall enforce the *Privileged User Creation SFP*[3] on:

Subjects: Privileged User

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

Creation	*Objects: New security attributes for the Privileged User to be created.* *Operations: Create_New_Privileged_User:* *The TOE creates R.Privileged_User and R.Reference_Privileged_User_Authentication_Data with information transmitted by Privileged User[4].*

Application Note 40

The ST writer shall describe how the initial Privileged User is created and if there are additional requirements for quorum of Privileged User to create a new Privileged User.

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

FDP_ACF.1.1/ Privileged User Creation	The TSF shall enforce the *Privileged User Creation SFP[5]* to objects based on the following: *(1) whether the subject is a Privileged User authorized to create a new Privileged User[6].*
FDP_ACF.1.2/ Privileged User Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User who has been authorised for creation of new users can carry out the Create_New_Privileged_User operation[7].*
FDP_ACF.1.3/ Privileged User Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None[8].*
FDP_ACF.1.4/ Privileged User Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None[9].*

The following security functional requirements in the FDP_ACC.1/ series Signer Creation, Signer Key Pair Generation, Signer Maintenance, Supply DTBS/R and Signing are intended as building blocks for the ST writer to describe Signer management and the signature operation within the TOE for long and one-time keys.

FDP_ACC.1/Signer Creation	Subset access control

FDP_ACC.1.1/	The TSF shall enforce the *Signer Creation SFP[10]* on:

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

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

[6] [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*]

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

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

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

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

Signer Creation	*Subjects: Privileged User* *Objects: R.Signer and R.Reference_Signer_Authentication_Data* *Operations: Create_New_Signer[11].* *The TOE creates R.Signer and R.Reference_Signer_Authentication_Data with information transmitted by Privileged User[12]*

FDP_ACF.1/Signer Creation	Security attribute based access control

FDP_ACF.1.1/ Signer Creation	The TSF shall enforce the *Signer Creation SFP[13]* to objects based on the following: *(1) whether the subject is a Privileged User authorized to create a new Signer[14].*
FDP_ACF.1.2/ Signer Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User who has been authorised for creation of new users can carry out the Create_New_Signer operation[15].*
FDP_ACF.1.3/ Signer Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None[16].*
FDP_ACF.1.4/ Signer Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None[17].*

FDP_ACC.1/Signer Maintenance	Subset access control

FDP_ACC.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP[18]* on: *Subjects: Privileged User and Signer* *Objects: The security attributes R.Reference_Signer_Authentication_Data of R.Signer* *Operations: Signer_Maintenance:* *The Privileged User or Signer instructs the TOE to update* *R.Reference_Signer_Authentication_Data of R.Signer[19].*

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

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

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

[14] [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*]

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

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

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

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

FDP_ACF.1/Signer Maintenance	Security attribute based access control

FDP_ACF.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP*[20] to objects based on the following: *(1) Whether the subject is a Privileged User or Signer authorised to maintain the Signer security attributes*[21].
FDP_ACF.1.2/ Signer Maintenance	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User or Signer who has been authorised to maintain a Signer can carry out the Signer_Maintenance operation*[22]*.*
FDP_ACF.1.3/ Signer Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *(1) The Signer must be the owner of the R.Signer object to be maintained*[23]*.*
FDP_ACF.1.4/ Signer Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *(1) If the Signer does not own the R.Signer object, it can't be maintained*[24]*.*

Application Note 41

The ST writer shall describe if R.Reference_Signer_Authentication_Data can be maintained by both Privileged User and Signer.

FDP_ACC.1/Signer Key Pair Generation	Subset access control

FDP_ACC.1.1/ Signer Key Pair Generation	The TSF shall enforce the *Signer Key Pair Generation SFP*[25]: *Subjects: Privileged User and Signer.* *Objects: The security attributes R.SVD and R.Signing_Key_Id as part of R.Signer.* *Operations: Generate_Signer_Key_Pair:* *The Privileged User or Signer instructs 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*[26]*.*

---

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

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

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

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

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

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

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

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

Application Note 42

The ST writer shall describe how R.Authorisation_Data is established.

Application Note 43

The ST writer shall describe if signing keys can be used by several cryptographic modules and how the keys are protected outside the module, including a description of how the association to R.Signer and R.Authorisation_Data are maintained. See FDP_UCT.1.

Application Note 44

Signing keys may be generated by the Cryptographic Module in advance, as so called pre-generated keys, in order to improve performance. If the TOE uses pre-generated keys, the ST writer shall describe how these are protected before they are assigned to a Signer.

Application Note 45

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

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

FDP_ACF.1.1/ Signer Key Pair Generation	The TSF shall enforce the *Signer Key Pair Generation SFP*[27] to objects based on the following: *(1) whether the subject is a Privileged User or Signer authorised to generate a key pair*[28]*.*
FDP_ACF.1.2/ Signer Key Pair Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User or Signer who has been authorised to generate the key pair can carry out the Generate_Signer_Key_Pair operation*[29]*.*
FDP_ACF.1.3/ Signer Key Pair Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *(1) The Signer must be the owner of the R.Signer object where the key pair is to be generated*[30]*.*
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*[31]*.*

Application Note 46

If pre-generated keys are used then FDP_ACF.1.4/Signer Key Pair Generation shall prevent assigning an already assigned key pair to the R.Signer object.

Application Note 47

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

---

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

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

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

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

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

FDP_ACC.1/Signer Key Pair Deletion	Subset access control

FDP_ACC.1.1/ Signer Key Pair Deletion	The TSF shall enforce the *Signer Key Pair Deletion SFP*[32] on: *Subjects: Privileged User and Signer* *Objects: The security attributes R.Signing_Key_Id and R.SVD of R.Signer* *Operations: Signer_Key_Pair_Deletion:* *The Privileged User or Signer instructs the TOE to delete the R.Signing_Key_Id and R.SVD from R.Signer*[33]*.*

Application Note 48

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

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

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

FDP_ACF.1.1/ Signer Key Pair Deletion	The TSF shall enforce the *Signer Key Pair Deletion SFP*[34] to objects based on the following: *(1) Whether the subject is a Privileged User or Signer authorised to delete the Signer security attributes*[35].
FDP_ACF.1.2/ Signer Key Pair Deletion	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User or Signer who has been authorised to delete a key pair can carry out the Signer_Key_Pair_Deletion operation*[36]*.*
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*[37]*.*
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*[38]*.*

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

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

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

[35] [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*]

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

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

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

FDP_ACC.1/Supply DTBS/R	Subset access control

FDP_ACC.1.1/ Supply DTBS/R	The TSF shall enforce the *Supply DTBS/R SFP*[39] on: *Subjects: Privileged User* *Objects: The security attributes R.DTBS/R of R.Signer.* *Operations: Supply_DTBS/R:* *The Privileged User instructs the TOE to link the supplied DTBS/R(s) to the next signature operation for R.Signer*[40]*.*

Application Note 49

If the TOE does not provide facilities to supply the DTBS/R(s) then the relevant part of the SFR is trivially satisfied, and this should be stated in the ST.

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

FDP_ACF.1.1/ Supply DTBS/R	The TSF shall enforce the *Supply DTBS/R SFP*[41] to objects based on the following: *(1) Whether the subject is a Privileged User authorised to supply a DTBS/R(s)*[42]*.*
FDP_ACF.1.2/ Supply DTBS/R	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User who has been authorised to supply a DTBS/R(s) can carry out the Supply_DTBS/R operation*[43]*.*
FDP_ACF.1.3/ Supply DTBS/R	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[44]*.*
FDP_ACF.1.4/ Supply DTBS/R	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None*[45]*.*

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

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

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

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

[42] [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*]

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

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

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

Application Note 50

If the TOE does not provide facilities to supply the DTBS/R(s) then the relevant part of the SFR is trivially satisfied, and this should be stated in the ST.

FDP_ACC.1/Signing	Subset access control

FDP_ACC.1.1/ Signing

The TSF shall enforce the *Signing SFP*[46] on:

Subjects: Signer

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

Operations: *Signing:*

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

- *The TOE establishes R.Authorisation_Data for the R.Signing_Key_Id.*
- *The TOE uses the R.Authorisation_Data, and R.Signing_Key_Id to activate a signing key in the Cryptographic Module and signs the R.DTBS/R resulting in R.Signature.*
- *The TOE deactivates the signing key when the signature operation is completed*[47]*.*

Application Note 51

The ST writer shall describe how R.Authorisation_Data is used to activate signing keys in the Cryptographic Module.

Application Note 52

The ST writer shall describe how the DTBS/R(s) is supplied to the TOE. It can be either in this function or using FDP_ACC.1/Supply DTBS/R.

Application Note 53

Signing key deactivating means that the signer shall authorise any subsequent use of it.

FDP_ACF.1/Signing	Security attribute based access control

FDP_ACF.1.1/ Signing

The TSF shall enforce the *Signing SFP*[48] to objects based on the following:

(1) Whether the subject is a Signer authorised to create a signature[49]*.*

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.

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

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

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

[49] [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*]

(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[50].

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[51].

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

(1) If the Signer does not own the R.Signer object, it can't be used to create a signature[52].

Application Note 54

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

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

FDP_ACC.1/TOE Maintenance	Subset access control

FDP_ACC.1.1/ TOE Maintenance — The TSF shall enforce the *TOE Maintenance SFP[53]* on:

Subjects: Privileged User

Objects: R.TSF_DATA.

Operations: TOE_Maintenance:

The Privileged User transmits information to the TOE to manage R.TSF_DATA [54].

FDP_ACF.1/TOE Maintenance	Security attribute based access control

FDP_ACF.1.1/ TOE Maintenance — The TSF shall enforce the *TOE Maintenance SFP[55]* to objects based on the following:

(1) Whether the subject is a Privileged User authorised to maintain the TOE configuration data[56].

---

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

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

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

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

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

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

[56] [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/ TOE Maintenance	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User who has been authorised to maintain the TOE can carry out the TOE_Maintenance operation[57].*
FDP_ACF.1.3/ TOE Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None[58].*
FDP_ACF.1.4/ TOE Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None[59].*

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

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

FDP_ETC.2.1/ Signer	The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion SFP, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP[60]* when exporting user data, controlled under the SFP(s), outside of the TSF.
FDP_ETC.2.2/ Signer	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/ Signer	The TSF shall ensure that the security attributes, when exported outside the TSF, are unambiguously associated with the exported user data.
FDP_ETC.2.4/ Signer	The TSF shall enforce the following rules when user data is exported from the TSF: *None[61]*.

Application Note 55

The ST writer shall describe which user data that can be exported from the TOE.

FDP_IFC.1/Signer	Subset information flow control

FDP_IFC.1.1/ Signer	The TSF shall enforce the *Signer Flow SFP[62]* on *Privileged User and Signer accessing Signer security attributes for all operations[63]*.

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

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

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

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

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

[62] [assignment: *information flow control SFP*]

[63] [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

FDP_IFF.1.1/ Signer	The TSF shall enforce the *Signer Flow SFP*[64] based on the following types of subject and information security attributes: *Privileged User and Signer accessing the Signer security attributes*[65].
FDP_IFF.1.2/ Signer	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance.* *To allow a Signer to sign, the Signer shall be created in the TOE by FDP_ACC.1/Signer Creation followed by FDP_ACC.1/Signer key Pair Generation.* *After Signer is created the following operations can be done: FDP_ACC.1/Signer Key Pair Generation, FDP_ACC.1/Signer Key Pair Deletion, FDP_ACC.1/Supply DTBS/R, FDP_ACC.1/Signer Maintenance and FDP_ACC.1/Signing*[66].
FDP_IFF.1.3/ Signer	The TSF shall enforce the: *None*[67].
FDP_IFF.1.4/ Signer	The TSF shall explicitly authorise an information flow based on the following rules: *None*[68].
FDP_IFF.1.5/ Signer	The TSF shall explicitly deny an information flow based on the following rules: *None*[69].

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

FDP_ETC.2.1/ Privileged User	The TSF shall enforce the *Privileged User Creation SFP*[70] when exporting user data, controlled under the SFP(s), outside of the TSF.
FDP_ETC.2.2/ Privileged User	The TSF shall export the user data with the user data's associated security attributes.
FPP_ETC.2.3/ Privileged User	The TSF shall ensure that the security attributes, when exported outside the TSF, are unambiguously associated with the exported user data.
FDP_ETC.2.4/ Privileged User	The TSF shall enforce the following rules when user data is exported from the TSF: *None*[71].

Application Note 56

The ST writer shall describe which user data that can be exported from the TOE.

[64] [assignment: *information flow control SFP*]

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

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

[67] [assignment: *additional information flow control SFP rules*]

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

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

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

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

FDP_IFC.1/Privileged User	Subset information flow control

FDP_IFC.1.1/ Privileged User	The TSF shall enforce the *Privileged User Flow SFP*[72] on *Privileged User accessing Privileged User security attributes for all operations*[73].

FDP_IFF.1/Privileged User	Simple security attributes

FDP_IFF.1.1/ Privileged User	The TSF shall enforce the *Privileged User Flow SFP*[74] based on the following types of subject and information security attributes: *Privileged User accessing the Privileged User security attributes*[75].
FDP_IFF.1.2/ Privileged User	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance*[76]*.*
FDP_IFF.1.3/ Privileged User	The TSF shall enforce the: *None*[77].
FDP_IFF.1.4/ Privileged User	The TSF shall explicitly authorise an information flow based on the following rules: *None*[78]*.*
FDP_IFF.1.5/ Privileged User	The TSF shall explicitly deny an information flow based on the following rules: *None*[79].

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

FDP_ITC.2.1/ Signer	The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP*[80] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/ Signer	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/ Signer	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/ Signer	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

[72] [assignment: *information flow control SFP*]

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

[74] [assignment: *information flow control SFP*]

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

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

[77] [assignment: *additional information flow control SFP rules*]

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

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

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

FDP_ITC.2.5/ Signer	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *None*[81].

Application Note 57

The ST writer shall describe which user data that can be imported to the TOE.

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

FDP_ITC.2.1/ Privileged User	The TSF shall enforce the *Privileged User Creation SFP*[82] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/ Privileged User	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/ Privileged User	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/ Privileged User	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/ Privileged User	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *None*[83].

Application Note 58

The ST writer shall describe which user data that can be imported to the TOE.

FDP_UCT.1	Basic data exchange confidentiality

FDP_UCT.1.1	The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP* [84] to *transmit and receive*[85] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1	Data exchange integrity

FDP_UIT.1.1	The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP* [86] to *transmit and receive*[87] user data in a manner protected from *modification and insertion*[88] errors **for R.Signer and R.Privileged User and for R.SAD also**[89] from *modification and replay*[90] errors.

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

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

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

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

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

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

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

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

[89] The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion and insertion*[91] **for R.Signer and R.Privileged_User and for R.SAD**[92] *whether modification and replay*[93] has occurred.

Application Note 59

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

8.4.4 Identification and Authentication (FIA)

FIA_AFL.1	Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number*], ***a TOE Maintenance***[94] configurable positive integer within [assignment: *range of acceptable values]*] unsuccessful authentication attempts occur related to *Privileged User and Signer authentication*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[95], the TSF shall *suspend the Privileged User and when it is a Signer suspend the usage of R.Signing_Key_Id*[96].

Application Note 60

The ST writer may extend FIA_AFL.1 to introduce operations to unsuspend Privileged Users or Signers.

Application Note 61

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

FIA_ATD.1	User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: *the security attribute as defined in FIA_USB.1*[97].

FIA_UAU.1	Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated

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

---

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

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

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

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

[94] *an administrator*

[95] [selection: *met, surpassed*]

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

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

FIA_UAU.5/Signer	Multiple authentication mechanisms

FIA_UAU.5.1/Signer **The TSF shall provide [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]*] to support Signer authentication**[98].

FIA_UAU.5.2/Signer The TSF shall authenticate any **Signer's[99]** claimed identity according to: **[selection: *[assignment: the rules describing how delegated authentication is verified by the TSF], [assignment: the rules describing how direct authentication mechanisms provide authentication]*][100]**.

Application Note 62

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

The ST writer shall list all the authentication factors type used to authenticate signer in accordance with [EN 419 241-1]. In particular, the ST writer shall include rules for authentication as part of SAD verification, as in FDP_ACF.1.2/Signing when delegated parties are used to assert the Signer's identity.

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

FIA_UAU.5/Privileged User	Multiple authentication mechanisms

FIA_UAU.5.1/Privileged User The TSF shall provide [assignment: *list of authentication mechanisms*] to support **Privileged User[101]** authentication.

FIA_UAU.5.2/Privileged User The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

FIA_UID.2	User identification before any action

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

FIA_USB.1	User-subject binding

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

(1) R.Reference_Signer_Authentication_Data

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

[99] user

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

[101] user

(2) *R.Signing_Key_Id*
(3) *R.SVD*
(4) *R.Signer*
(5) *[assignment: list of user security attributes]*

to Signer

(1) *R.Reference_Priviliged_User_Authentication_Data*
(2) *[assignment: list of user security attributes]*

to Privileged User[102].

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 authorized to create a new Signer.
(2) *Whether the subject is a Privileged User authorized to create a new Privileged User.*
(3) [assignment: *rules for the initial association of attributes*][103]*.*

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

(1) Whether the subject is a Privileged User authorized to modify an R.Signer object.
(2) *Whether the subject is a Signer authorized to modify his own R.Signer object.*
(3) [assignment: *rules for the changing of attributes*][104]*.*

Application Note 63

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

Application Note 64

The ST writer may include the R.Authrorisation_Data as a security attribute of the Signer.

Application Note 65

The ST writer shall describe if R.DTBS/R is a Signer attribute. This is expected if a Privileged User and not the Signer submits it to the TOE.

8.4.5 Security Management (FMT)

FMT_MSA.1/Signer	Management of security attributes

FMT_MSA.1.1/ Signer The TSF shall enforce the

(1) Signer Creation SFP[105] to restrict the ability to *create*[106] the security attributes *listed in FIA_USB.1 for Signer*[107] to *authorised Privileged User*[108]*.*

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

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

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

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

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

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

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

(2) *Generate Signer Key Pair SFP*[109] to restrict the ability to *generate*[110] the security attributes *R.SVD and R.Signing_Key_Id*[111] to *authorised Privileged User and Signer*[112].
(3) *Signer Key Pair Deletion SFP*[113] to restrict the ability to *destruct*[114] the security attribute *R.SVD and R.Signing_Key_Id as part of R.Signer*[115] to *authorised Signer*[116]
(4) *Supply DTBS/R SFP*[117] to restrict the ability to *create*[118] the security attribute *R.DTBS/R as part of R.Signer*[119] to *authorised Privileged User*[120]
(5) *Signing SFP*[121] to restrict the ability to *create*[122] the security attribute *R.DTBS/R as part of R.Signer* to *authorised Signer*[123].
(6) *Signing SFP*[124] to restrict the ability to *query*[125] *the security attributes as listed in FIA_USB.1* to *authorised Signer*[126].
(7) *Signer Maintenance SFP*[127] to restrict the ability to *change*[128] the security attributes *R.Reference_Signer_Authentication_Data*[129] *as part of R.Signer* to *authorised Privileged User and Signer*[130].

FMT_MSA.1/Privileged User	Management of security attributes

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

(1) *Privileged User Creation SFP*[131] to restrict the ability to *create and query*[132] the security attributes *listed in FIA_USB.1 for Privileged User*[133] to *authorised Privileged User*[134].

---

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

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

111 [assignment: *list of security attributes*]

112 [assignment: *the authorised identified roles*]

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

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

115 [assignment: *list of security attributes*]

116 [assignment: *the authorised identified roles*]

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

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

119 [assignment: *list of security attributes*]

120 [assignment: *the authorised identified roles*]

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

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

123 [assignment: *the authorised identified roles*]

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

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

126 [assignment: *the authorised identified roles*]

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

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

129 [assignment: *list of security attributes*]

130 [assignment: *the authorised identified roles*]

FMT_MSA.2	Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *all security attributes listed in FIA_USB.1*[135].

FMT_MSA.3/Signer	Static attribute initialisation

FMT_MSA.3.1/ Signer The TSF shall enforce the *Signer Creation SFP*[136] to provide *restrictive*[137] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ Signer The TSF shall allow the *Privileged User*[138] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Privileged User	Static attribute initialisation

FMT_MSA.3.1/ Privileged User The TSF shall enforce the *Privileged User Creation SFP*[139] to provide *restrictive*[140] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ Privileged User The TSF shall allow the *Privileged User*[141] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1	Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *modify*[142] the *R.TSF_DATA*[143] data to *Privileged User*[144].

Application Note 66

The TSF data includes configuration of administrator roles.

---

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

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

133 [assignment: *list of security attributes*]

134 [assignment: *the authorised identified roles*]

135 [assignment: *list of security attributes*]

136 [assignment: *access control SFP, information flow control SFP*]

137 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

138 [assignment: *the authorised identified roles*]

139 [assignment: *access control SFP, information flow control SFP*]

140 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

141 [assignment: *the authorised identified roles*]

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

143 [assignment: *list of TSF data*]

144 [assignment: *the authorised identified roles*]

FMT_SMF.1 Specification of Management Functions

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

(1) Signer management,
(2) Privileged User management,
(3) Configuration management,
(4) [assignment: additional list of management functions to be provided by the TSF][145].

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: *Signer and Privileged User,* [assignment: *other authorised identified roles*][146].

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*[147] are satisfied.

Application Note 67

The ST writer shall describe which roles are defined in the TOE and which operations the role can perform.

8.4.6 Protection of the TSF (FPT)

FPT_PHP.1 Passive

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

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

Application Note 68

Passive detection of a physical attack is typically achieved by using physical seals and an appropriate physical design of the TOE that allows the TOE administrator to verify the physical integrity of the TOE as part of a routine inspection procedure.
Because of the requirement for a physically secure environment with regular inspections (cf. OE.ENV), the level of protection (and hence resistance to attack potential) that is required by the implementation of FPT_PHP.1 for this TOE is equivalent to the physical security mechanisms for tamper detection and response required by section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements for each physical security embodiment in [ISO/IEC 19790] for Security Level 3.

FPT_PHP.3 Resistance

[145] [assignment: *list of management functions to be provided by the TSF*]

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

[147] [assignment: *conditions for the different roles*]

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the SFRs are always enforced.

Application Note 69

If the TOE is implemented as a local application within the same physical boundary as the cryptographic module defined in [EN 419-221-5] the SFRs FTP_PHP.* can rely on the similar SFRs described in the ST for the cryptographic module. Details should be stated in the Security Target.

Application Note 70

This SFR is linked to the requirements for passive detection of physical attacks in FPT_PHP.1, and should identify the relevant responses of the TOE involved in meeting the key zeroisation requirements of [ISO/IEC 19790] Security Level 3. As in the case of FPT_PHP.1, because of the requirement for a physically secure environment with regular inspections (cf. OE.ENV), the level of protection (and hence resistance to attack potential) that is required by the implementation of FPT_PHP.3 for this TOE is equivalent to the level of assessment for this aspect of tamper detection and response required for section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements by each physical security embodiment in [ISO/IEC 19790] for Security Level 3.

FPT_RPL.1	Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *R.SAD*[148]*.*

FPT_RPL.1.2 The TSF shall perform *reject the signature operation*[149] when replay is detected.

FPT_STM.1	Reliable time stamps

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

Application Note 71

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

FPT_TDC.1	Inter-TSF basic TSF data consistency

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

(1) R.Signer,
(2) R.Reference_Signer_Authentication_Data,
(3) R.SAD,
(4) R.DTBS/R
(5) R.SVD
(6) R.Privileged_User
(7) R.Reference_Privileged_User_Authentication_Data
(8) R.TSF_DATA[150]

when shared between the TSF and another trusted IT product.

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

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

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

FPT_TDC.1.2 The TSF shall use *data integrity either on data or on communication channel*[151] when interpreting the TSF data from another trusted IT product.

Application Note 72

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

8.4.7 Trusted Paths/Channels (FTP)

FTP_TRP.1/SSA	Inter-TSF Trusted path

FTP_TRP.1.1/SSA The TSF shall provide a communication path between itself and ***Privileged User through SSA***[152] 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*[153].

FTP_TRP.1.2/SSA The TSF shall permit ***Privileged User through SSA***[154] to initiate communication via the trusted path.

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

(1) FDP_ACC.1.1/Privileged User Creation
(2) FDP_ACC.1/Signer Creation
(3) FDP_ACC.1/Signer Maintenance
(4) FDP_ACC.1/Signer Key Pair Generation
(5) FDP_ACC.1/Signer Key Pair Deletion
(6) FDP_ACC.1/Supply DTBS/R
(7) FDP_ACC.1/TOE Maintenance
(8) [assignment: other services for which trusted path is required][155].

Application Note 73

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

FTP_TRP.1/SIC	Inter-TSF Trusted path

FTP_TRP.1.1/SIC The TSF shall provide a communication path between itself and ***Remote Signer through the SIC***[156] 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*[157].

FTP_TRP.1.2/SIC The TSF shall permit ***Remote Signer through SIC***[158] to initiate communication via the trusted path.

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

---

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

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

[153] [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]

[154] [selection: *the TSF, local users, remote users*]

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

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

[157] [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]

[158] [selection: *the TSF, local users, remote users*]

(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) *[assignment: other services for which trusted path is required]*[159].

Application Note 74

Since it is not all data transmitted to the TOE that needs to be protected in confidentiality, FTP_TRP.1.1/SIC only requires protection from modification. The ST writer shall describe if the SAP can be used to transmit sensitive data and how these are protected in confidentiality.

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

FTP_ITC.1.1/CM The TSF shall provide a communication path between itself and **a cryptographic module certified according to [EN 419 221-5]*[160]*** that is logically distinct from other communication paths and provides assured authentication of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2/CM The TSF shall permit **the TSF and a cryptographic module certified according to [EN 419 221-5]**[161] to initiate communication via the trusted channel.

FTP_ITC.1.3/CM The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note 75

FTP_ITC.1/CM must be completed in a Security Target to reflect the way that the TOE communicates with the cryptographic module, and to justify its security. Where the TOE and the cryptographic module are located within the same hardware appliance (e.g. the TOE being a local application running on a server and communicating with a PCI card on the server's internal PCI bus) then the trusted channel may be mapped in the Security Target to the physical configuration, and no additional authentication or cryptographic protection are required (because of the physical security assumed in the appliance environment).

8.5 Security Assurance Requirements

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

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

Assurance Class	**Assurance Components**
Development (ADV)	Security architecture description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.4)
	Implementation representation of the TSF (ADV_IMP.1)

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

[160] another trusted IT product

[161] [selection: *the TSF, another trusted IT product*]

Assurance Class	Assurance Components
	Basic modular design (ADV_TDS.3)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability assessment (AVA)	**Advanced methodical vulnerability analysis** (**AVA_VAN.5**)

Table 12

9 Rationale

9.1 Security Requirements Rationale

9.1.1 Security Requirements Coverage

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

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
Security Audit																	
FAU_GEN.1										X							
FAU_GEN.2										X							
Cryptographic Support																	
FCS_CKM.1			X													X	
FCS_CKM.4			X														
FCS_COP.1			X												X	X	
FCS_RNG.1			X														X
User Data Protection																	
FDP_ACC.1/ Privileged User Creation					X												
FDP_ACF.1/ Privileged User Creation					X												
FDP_ACC.1/ Signer		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
Creation																	
FDP_ACF.1/ Signer Creation		X						X									
FDP_ACC.1/ Signer Maintenance		X															
FDP_ACF.1/ Signer Maintenance		X															
FDP_ACC.1/ Signer Key Pair Generation			X	X													
FDP_ACF.1/ Signer Key Pair Generation			X	X													
FDP_ACC.1/ Signer Key Pair Deletion								X									
FDP_ACF.1/ Signer Key Pair Deletion								X									
FDP_ACC.1/ Supply DTBS/R														X			
FDP_ACF.1/ Supply DTBS/R														X			
FDP_ACC.1/											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
Signing																	
FDP_ACF.1/ Signing											X				X		
FDP_ACC.1/ TOE Maintenance									X								
FDP_ACF.1/TOE Maintenance									X								
FDP_ETC.2/ Signer	X																
FDP_IFC.1/Signer	X																
FDP_IFF.1/Signer	X																
FDP_ETC.2/ Privileged User					X		X										
FDP_IFC.1/Privileged User					X		X										
FDP_IFF.1/privileged User					X		X										
FDP_ITC.2/Signer	X																
FDP_ITC.2/Privileged User					X		X										
FDP_UCT.1	X																
FDP_UIT.1	X																
Identification																	

	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
and Authentication																	
FIA_AFL.1						X					X						
FIA_ATD.1	X				X		X										
FIA_UAU.1						X					X						
FIA_UAU.5/Signer											X						
FIA_UAU.5/Privileged User						X											
FIA_UID.2					X		X	X									
FIA_USB.1	X		X		X		X										
Security Management																	
FMT_MSA.1/ Signer								X									
FMT_MSA.1/ Privileged User					X			X									
FMT_MSA.2					X			X									
FMT_MSA.3/ Signer								X									
FMT_MSA.3/ Privileged User					X			X									
FMT_MTD.1									X								
FMT_SMF.1									X								
FMT_SMR.2									X								

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
Protection of the TSF																	
FPT_PHP.1									X								
FPT_PHP.3									X								
FPT_RPL.1												X					
FPT_STM.1										X							
FPT_TDC.1	X				X												
Trusted Path/Channels																	
FTP_TRP.1/SSA									X					X			
FTP_TRP.1/SIC												X	X	X			
FTP_ITC.1/CM			X												X		

Table 13

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_Authenticaton_Data.

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

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

OT.PRIVILEGED_USER_MANAGEMENT is handled by requirements for export and import of R.Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/privileged User, FDP_ITC.2/Privileged User and FPT_TDC.1). 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, FIA_UAU.1 and FIA_UAU.5/Privileged User.

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

OT.SYSTEM_PROTECTION is handled by FMT_MTD.1, FMT_SMF.1 and FMT_SMR.2. FDP_ACC.1/TOE Maintenance and FDP_ACF.1/TOE Maintenance describes access control rules for managing TSF data. FPT_PHP.1 and FPT_PHP.3 describes requirements for TSF protection. FTP_TRP.1/SSA describes that only a Privileged User can maintain the TOE.

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

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

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

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

OT.DTBSR_INTEGRITY is covered by FTP_TRP.1/SSA and FTP_TRP.1/SIC requiring data transmission to be protected in integrity.

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

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

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

9.2 SFR Dependencies

The dependencies between SFRs are addressed as shown in

Requirement	Dependencies	Fullfilled 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	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1
FCS_RNG.1	None	No 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 Maintenance	FDP_ACF.1	FDP_ACF.1/Signer Maintenance
FDP_ACC.1/Signer Key Pair Generation	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Generation
FDP_ACC.1/Signer Key Pair Deletion	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Deletion
FDP_ACC.1/Supply DTBS/R	FDP_ACF.1	FDP_ACF.1/Supply DTBS/R
FDP_ACC.1/Signing	FDP_ACF.1	FDP_ACF.1/Signing
FDP_ACC.1/TOE Maintenance	FDP_ACF.1	FDP_ACF.1/TOE Maintenance

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

Requirement	Dependencies	Fullfilled by
		FDP_IFC.1/Privileged User
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FTP_TRP.1/SSA and FTP_TRP.1/SIC
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5/Signer	None	
FIA_UAU.5/Privileged User	None	
FIA_UID.2	None	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1/Signer	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Signer FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/Privileged User	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Privileged User FMT_SMR.2 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FMT_MSA.1/Signer FMT_MSA.1/Privileged User FMT_SMR.2
FMT_MSA.3/Signer	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Signer FMT_SMR.2
FMT_MSA.3/Privileged User	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Privileged FMT_SMR.2
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_SMF.1	None	
FMT_SMR.2	FIA_UID.1	FIA_UID.2
FPT_PHP.1	None	
FPT_PHP.3	None	
FPT_RPL.1	None	
FPT_STM.1	None	
FPT_TDC.1	None	
FTP_TRP.1/SSA	None	
FTP_TRP.1/SIC	None	

Requirement	Dependencies	Fullfilled by
FTP_ITC.1/CM	None	

Table 14

9.2.1 Rationales for SARs

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

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

EAL4 is therefore augmented with AVA_VAN.5.

Bibliography

[eIDAS] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[Assurance] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

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

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 4. CCMB-2012-09-002, September 2012.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4. CCMB-2012-09-002, September 2012.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4. CCMB-2012-09-003, September 2012.

[EN 419 241-1] CEN/TS 419 241-1 Security Requirements for Systems Supporting Server Signing. Draft.

[EN 419 221-5] CEN/PP 419 221-5 Protection Profiles for TSP Cryptographic modules – Part 5, Cryptographic Modules for Trust Services.

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

[ETSI TS 119 312] ETSI, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. 2014.

[ETSI EN 319 401] ETSI, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, 2016.

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

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