Protection Profile for Signature Activation Protocol (SAP) management

Emission Date : 15 January 2016
Ref./Version : PP-SAP/1.4
Number of pages : 103 (including two header pages)

Table of Contents

Table of Figures

Table of Tables

1 PP 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” summarizes the PP in narrative form. Section 1.3 "TOE Overview" summarizes 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.

1.1 PP Reference

Title: Protection Profile for Signature Activation Protocol (SAP) management
Sponsor: ANSSI
CC Version: 3.1 (Revision 4)
Assurance Level: The minimum assurance level for this PP is EAL4 augmented.
General Status: Evaluated
Version Number: 1.4

Keywords: EIDAS, Server signing, Sole Control Component, Qualified signature, remote signature creation device RSCD

1.2 Protection Profile Overview

This Protection Profile (PP) defines the security requirements of a software used as Sole Control Component (SCC) running on a Platform and used as part of their infrastructure for Trustworthy System Supporting Server Signing (TW4S) that generate advanced electronic signatures as defined in [REGULATION].

System overview is given in TOE overview chapter.

In order to provide confidence in TW4S, it is required to provide a set of Common Criteria evaluated components consisting in:

- A Trustworthy Signature Creation Module (TSCM), conformant to the TSCM protection profile which is defined by [PP TSCM].
- A cryptographic module conformant to the SAP HSM protection profile which is defined by [PP SAP HSM].
- A software named Sole Control Component (SCC), conformant to this document which is defined by [PP SAP].

This PP is Common Criteria Part 2 extended and Common Criteria Part 3 conformant. The assurance level for this PP is EAL4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_DVS.2 (Development Security).

As shown on figure 1, this document focuses on the security requirements for only the SCC software. Assumptions A.TSCM_CERTIFIED and A.SAP_HSM_CERTIFIED are defined to be assured that such items in the Remote Environment are evaluated according to identified protection profiles.

This protection profile does not require formal compliance to any specific protection profiles but recommended protection profiles can be found in appendix according to examples of potential product configurations.

1.3 European Legislation

The software on device used as Sole Control Component certified according to this PP participate to meet the security assurance requirements of European legislation as defined in [REGULATION].

2 TOE Overview

2.1 System Overview

The TOE is part of a TW4S working within a not controlled local environment to signatory as shown on next figure. The TW4S will operate running on a networked server in order to allow one or more signatories to remotely sign electronic documents using centralized signature keys held on the signing server under sole control of the signatory, and responding to the security requirements described in part 1 of [EN-419241].

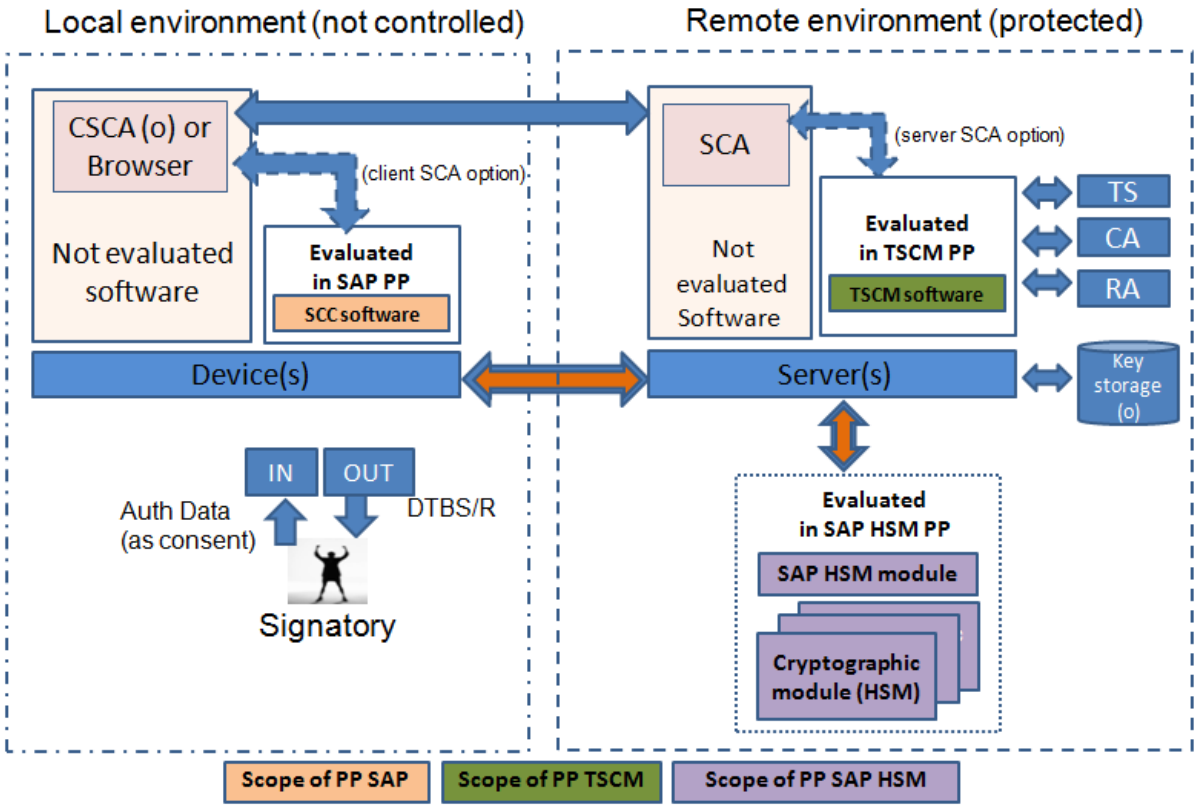


Figure 1 - System overview and PP scope

The figure 1 represent a logical view of the system including:

- in remote (also named SERVER-SIDE) environment (not in this PP evaluation scope) :
    - Signature Creation Application (including server part SCA connected to local part to signatory using a browser or client part also named CSCA), initiating signature request,
    - Trustworthy Signature Creation Module (also named TSCM) conformant to [PP TSCM] to manage signature request,
    - A SAP HSM module (certified in composite evaluation on HSM certified according to CEN 419221-5) conformant to [PP SAP HSM] to perform access control to signature operation performed by cryptographic module (HSM) conformant to [CEN 419221-5] to perform signature operation on behalf of signatory, and
    - Additional software (Time Source (TS), Certification Authority, Registration Authority),
- and in local (also named HOLDER-SIDE) environment:

- browser or Client Signature Creation Application (also named CSCA), and additional software not in evaluation scope,
- Sole Control Component (also named SCC) conformant to this PP to achieve steps in sole control of signature operation by the signatory,
- Means to exchange with signatory for data entry (IN) and display (OUT).

Note: Server(s) means that applications can be located on same server or not with an optional connection with logical or physical secure link.

Note: Device(s) means that applications can be located on same device or not with an optional connection with logical or physical secure link.

Note that SAP HSM module and the TSCM software will be fully described in associated security targets conformant to [PP SAP HSM] and [PP TSCM] respectively.

The system as a whole must:

- Ensure that the data to be signed (DTBS) used as input of the signature process has been actually seen or selected by the signatory,
- Ensure that the authentication of the signatory (using direct signatory verification data check by SERVER-SIDE part or HOLDER-SIDE check by SCC and SCC authentication to SERVER (TSCM or SAP HSM) on behalf of signatory),
- Ensure that the Signatory's SCD on the server is activated only after the signatory authentication and the link between the Signatory authentication, the SCD to be used and the DTBS have been validated.

These steps must be done in a way protecting against Signatory authentication on SCC reuse and ensuring integrity and confidentiality of DTBS and signature result.

2.2 Protection Profile Scope vs Security Target Scope

As shown on Figure 3, this Protection Profile focuses on the security requirements for the SCC and considers the underlying Platform running SCC as the environment of the TOE, thus covered by security objectives. Nevertheless, any product evaluation against this PP shall include the items of the platform:

- Integrated circuit (IC) and its Dedicated Software (DS),
- Operated System (OS) and its Run Time Environment (RTE),

and the SCC software.

This PP does not require formal compliance to any specific Protection Profiles but recommended PPs can be found in appendix according to examples of potential product configurations.

This Protection Profile requires "Demonstrable" conformance.

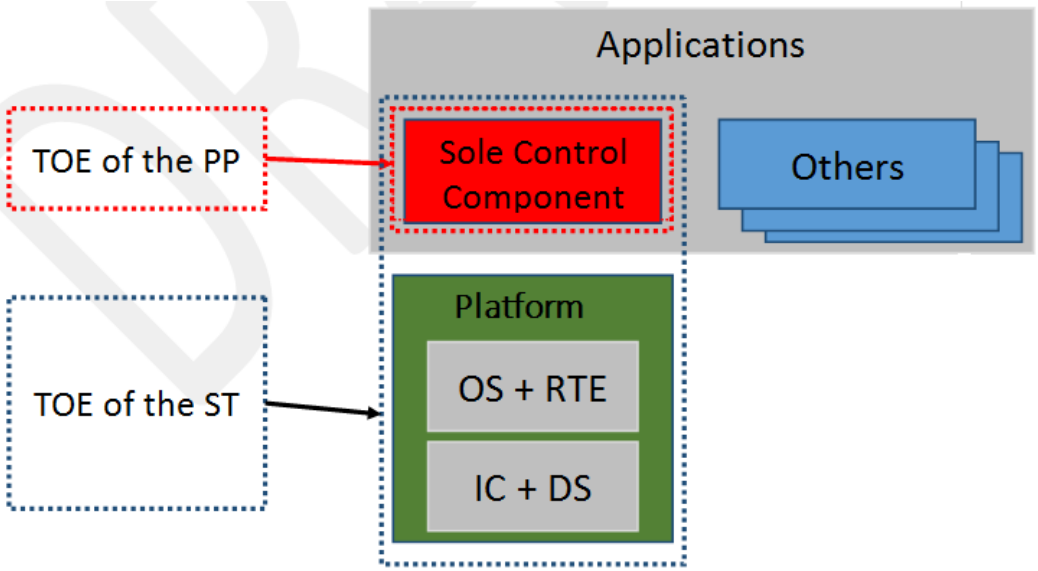


Figure 2 - PP and ST scope

2.3 TOE type

The TOE is the Sole Control Component (SCC) as described in red in Figure 3.
TOE is designed to provide sole control to signatory on remote signature operation requested by TSCM to SAP HSM. More precisely, SAP HSM only authorizes signatory operation based on verification of SAD provided by SCC.
TOE provides means to signatory to be authenticated by the TSCM and to create a secure channel with TSCM. TOE participates to the signature activation protocol shared with the Trustworthy Signature Creation Module (TSCM) and SAP HSM.

2.4 TOE Environments

Figure 4 illustrates the different environments for TOE:

- Enrolment environment (where SCC is enroled in TW4S),
- Management environment (where SCC is administrated [remotely or in secure environment]),
- Operational environment (where SCC is used for signature operation).

Note: Development and Manufacturing environment (SCC software is developed and associated to hardware) is not covered by the figure.

A different interface is provided to associated roles in each environment.

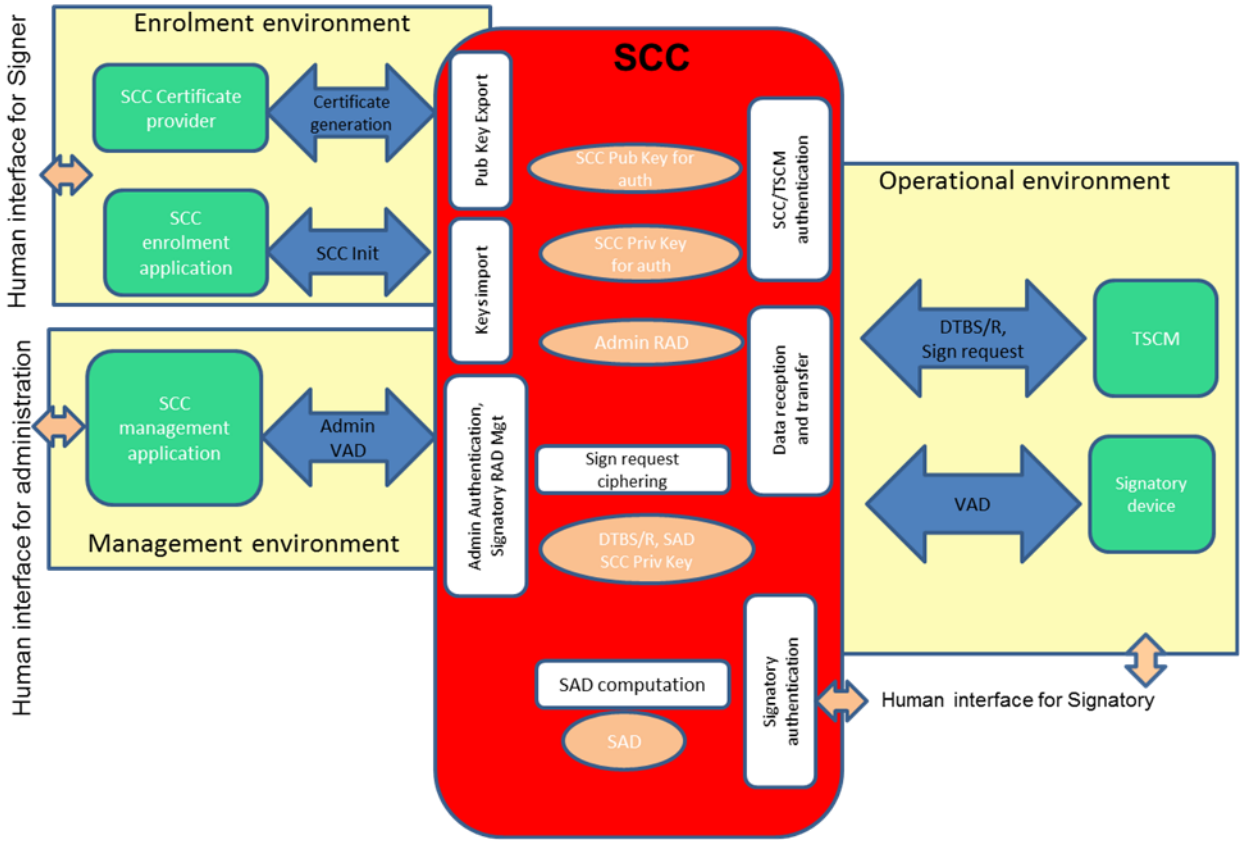


Figure 3 - TOE (in red) within its different environments

TOE provides different security services in each environment.
In operational environment, the two main functionalities are Authentication and Signature activation protocol detailed in TOE usage chapter.
In development and manufacturing environment, SCC software is not yet fully available to users. It provides a dedicated subset of administration features for issuer only.
In enrolment environment, main functions are associated to key and sensitive data initialization prior or after SCC delivery.
In management environment, main functions are associated sensitive data management requiring interaction with administrator after SCC delivery (as VAD or key update).

2.5 TOE Life Cycle

A generic life cycle is proposed in the following figure. It includes several phases as: SCC development, enrolment and usage.

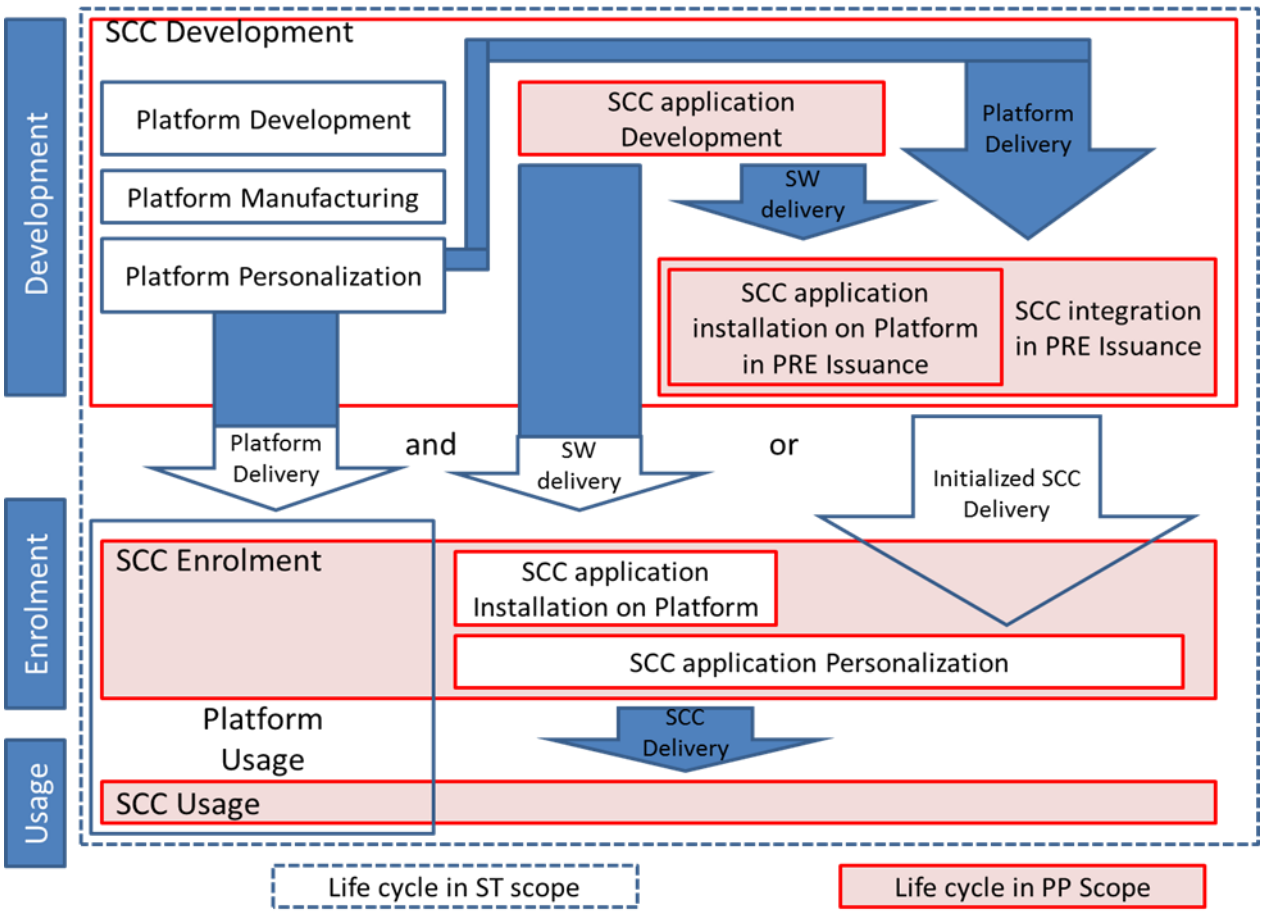


Figure 4 - TOE Life cycles

SCC development includes:

A) relevant activities for platform as development manufacturing and personalization,
B) SCC application development
C) SCC application installation on platform prior delivery by issuer (optional)

SCC enrolment includes:

D) SCC application installation on platform prior delivery by administrator (optional)
E) SCC application personalization by issuer

SCC usage includes:

F) SCC application usage on platform by signatory or administrator
G) SCC application blocking or deletion by administrator (if required)
H) platform blocking by administrator (if required)

2.5.1 Development and Manufacturing Environment

To be completed by ST writer.

2.5.2 Enrolment Environment

To be completed by ST writer.

2.5.3 Operational Environment

To be completed by ST writer.

2.5.4 Administration Environment

To be completed by ST writer.

2.6 TOE Usage and Group Organization

In operational environment, the two main functionalities are Authentication and Signature activation protocol.
The primary functionality of the TOE is to enable the Signatory to authenticate himself to TW4S, (by SCC using HOLDER-SIDE signatory authentication or by SAP HSM using remote signatory authentication) and authenticate SERVER (TSCM or SAP HSM) and provide information to be authenticated by SERVER. It also contributes to secure channel creation with SERVER, managing secure data transfer inside secure channel with SERVER.
The other main functionality is to contribute to signature activation protocol, by controlling access to SAD computation requiring prior signatory authentication and performing SAD computation and SAD transfer to SERVER.
All the functions are detailed in next chapters.
The operational environment of the TOE is considered as hostile therefore we consider attacker with ability to access to item similar to TOE or TOE to prepare and to perform physical attack on TOE.
Nevertheless, TOE is supposed to be under control of signatory during usage phase even if unwanted access by attacker is considered.

2.6.1 PP Configurations and Functional Groups

This protection profile is a modular PP as defined in [CCM]. It includes a base-PP that specifies the requirements mandatory for all configurations of products claiming conformance with this PP and module-PP specifying options only required in specific TOE configurations.
The module-PPs are available in the appendix of this document. Module-PPs are categorized in 2 categories:

- Optional modules that specify requirements that may be optionally included in the security target claiming conformance,
- Alternative modules when one of the alternative modules shall be included in the security target claiming conformance.

The groups are listed in the following table:

Module-PP Name	Type	Description
CORE GROUP	Mandatory	It proposes all main functions of TOE.
PRIVACY GROUP	Optional	It proposes all main functions linked to signatory privacy in TOE. It is associated to confidential of sensitive data linked to the DTBS or the signatory identity. This Group applies only if the TOE provides privacy protection functions
ADMINISTRATION GROUP	Optional	It proposes main optional administrative functions provided by TOE. This Group applies only if the TOE provides administrative functions during the usage phase
HOLDER-SIDE AUTHENTICATION GROUP	Alternative	It proposes Signatory authentication by SCC
SERVER-SIDE AUTHENTICATION GROUP	Alternative	It proposes Signatory authentication by SERVER

Table 1 - Module-PP Names and Types

Note that the optional groups ADMINISTRATION and PRIVACY are detailed in Appendices A and B, respectively.

Note that the alternative modules HOLDER-SIDE Authentication and SERVER-SIDE Authentication are detailed in Appendices C and D, respectively.

2.6.2 Cryptographic Functions of the TOE

The next paragraphs list the security functions provided by the TOE. When title is followed by bracket [], it means that security function is associated to a specific optional group otherwise, it is associated to core group. Such optional functions are described more deeply in appendixes.

SAP_HSM authentication by the TOE

This function allows the authentication of the SAP HSM by the TOE, to ensure that communication is not done with an unauthorized entity.

Note: TSCM authentication to ensure that communication is not done with an unauthorized entity is assumed by TOE environment which is not necessarily evaluated.

TOE authentication by the SAP_HSM

This function provides cryptographic evidence computed by for TOE transferred to SAP_HSM allowing TOE authentication by SAP _HSM and ensuring that communication is not done with an unauthorized entity.

Secure channel management by the TOE

This function allows the TOE to manage the creation of the secure channel with the SERVER (SAP HSM) to exchange securely data with such entities.
It includes functions to ensure confidentiality and integrity of sent or received data.

SAD generation on DTBS/R demonstrating sole control by signatory

This function generates the SAD to create the link between DTBS/R and signatory consent to use a SCD for a signature operation on this DTBS/R. The SAD expresses the Signatory consent to perform a signature operation on a given DTBS with a given identity and associated signing key.

Data Integrity secure transfer to the SERVER (here SAP HSM)

This function assumes that data exchanges are made between SCC and SERVER (using channel provided by TSCM) in a way keeping data integrity.

Note: Data Integrity and confidentiality secure transfer to the TSCM is assumed by TOE environment which is not necessarily evaluated.

Data confidentiality in secure transfer to the SERVER (SAP HSM) [Privacy group only]

This function assumes that data exchanges are made between SCC and SERVER in a way keeping data (as D.DTBSR_C, D.IDENTIFICATION_DATA_C) confidentiality. It is applicable only when required.

2.6.3 Security Functions of the TOE

Access control by the TOE to security functions authorized only to Signatory

This function performs the access control to security functions requiring user to be authenticated as Signatory prior to access to the set of functions reserved to the Signatory.

Import Signatory ID
This function allows importation of Signatory identifier.

Import SCD ID
This function allows importation of SCD identifier.

Import Signatory Data
This function allows importation of Signatory data used for SAD computation (if required)

Signatory RAD importation during enrolment phase [HOLDER-SIDE Authentication group only]
This function allows the importation of the RAD dedicated to the Signatory in the TOE.
Such function is supposed to be done in a secure environment.

Protection of integrity of Signatory and SCC Data
Stored data integrity protection is managed by TOE and platform associated services.

Protection of confidentiality of Signatory and SCC Data
Stored data confidentiality protection is managed by TOE and platform associated services.

Signatory RAD replacement in usage phase [Administration group only]
This function allows the Signatory to replace the RAD after specific conditions are fulfilled.

Signatory Authentication by the TOE [HOLDER-SIDE Signatory Authentication group only]
This function allows the authentication of the Signatory by the TOE by presenting VAD to be compared with RAD stored in TOE.

Signatory Authentication data transfer from TOE to SERVER [SERVER-SIDE Signatory Authentication group only]
This function allows the transfer of Signatory authentication data (VAD) to the SERVER from TOE allowing SERVER to compare VAD with RAD stored in SERVER. Result of comparison is retrieved by SCC to consider Signatory as authenticated.

Administrator Authentication by the TOE [Administration group only]
This function allows the authentication of the administrator by the TOE by presenting administrator VAD to be compared with associated RAD stored in TOE.

Access control by the TOE to security functions authorized only to Administrator [Administration group only]
This function performs the access control to security functions requiring user to be authenticated as administrator prior to access to the set of functions reserved to administrator.

2.6.4 Key Management

The TOE supports the secure management of cryptographic keys (Symmetric and/or Asymmetric) associated to authentication of SCC and SERVER,

- with key generation and key exportation for SCC authentication, and /or
- with key importation for SCC authentication,
- with key importation for SERVER authentication,
- with SAD key importation for SAD computation,

In addition, key storage and handling is managed by TOE and platform associated services to keep key integrity and confidentiality.

3 Conformance Claims

3.1 CC Conformance Claim

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

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; [CEM]), has to be taken into account.

3.2 PP Claim

This Protection Profile does not require formal compliance to any specific Protection Profiles but recommended Protection Profiles can be found in appendix according to examples of potential product configurations.

3.3 Package Claim

This PP is conforming to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3[CC3].

3.4 Conformance Rationale

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

3.5 Conformance Statement

The conformance to this PP, required for the Security Targets and Protection Profiles claiming conformance to it, is demonstrable, as defined in CC Part 1. This would facilitate conformance claim to other PPs for Security Target (ST) authors.

The Security target claiming conformance to the PP must state which optional groups (HOLDER-SIDE_authentication, SERVER-SIDE authentication, administration, privacy) are claimed.

Note that the ST author must verify when claiming conformance with multiple optional groups (HOLDER-SIDE_authentication, SERVER-SIDE authentication, administration, privacy) that the integration of the PP Core module and all claimed PP optional modules into the ST complies with the rules specified by the [CC] for demonstrable conformance.

4 Security Problem Definition

4.1 Users / Subjects

This protection profile considers the following users (human or IT entity possibly interacting with the TOE from outside of the TOE boundary) and subjects (active entity in the TOE that performs operations on objects):

Issuer or CSP

During the personalization phase of the device, the authenticated Holder acts as the Issuer to perform the following operations:

- Authenticate himself with his own VAD to the TOE,
- Import the Issuer RAD into the TOE,
- Import the Authentication Protocol sensitive data into the TOE.
- Import the Authentication key into the TOE.
- Request an Authentication key generation inside the TOE
- Export the Authentication public key from the TOE in the case of use of Asymmetric Key pair for SCC authentication.
- Import the Administrator RAD into the TOE.

Holder

Holder is a generic role that can be used thereinafter in the document. It covers entity holding TOE in current operation authenticated as Issuer, Administrator and Signatory roles.

During the usage phase, the authenticated Holder acts as the Administrator or the Signatory. During the personalization phase, the authenticated Holder acts as the Issuer.

Signatory

Signatory is the legitimate user of the signature activation function as part of signature activation protocol. It is associated to the authenticated holder performing signature activation during the usage phase. The Signatory may perform the following operations:

- Authenticate himself by presenting his own VAD to TOE, or,
- Authenticate himself by providing his own VAD to SERVER using secure channel provided by TOE for secure transfer of VAD and result of authentication.

Administrator

During the usage phase of the TOE, the authenticated Holder acts as the Administrator to perform the following operations:

- authenticate himself with his own VAD to the TOE,
- change the Signatory RAD into the TOE [administration group only],
- import the Authentication Protocol sensitive data into the TOE,
- block usage of signature activation function (if required).

Signatory Device

A Signatory Device is any technical system communicating with the TOE through the interface to interact with signatory. It is considered as user environment interacting with SERVER (TSCM).

SERVER (TSCM or SAP HSM):

TSCM

A Trustworthy Signature Creation Module is a technical system, connected to Signature Creation Application (SCA), used to provide SERVER-SIDE TOE authentication and operation for signature activation protocol and service. It is considered as user environment.

SAP HSM

SAP HSM is a local application hosted in HSM providing user authentication function and flexible authorization function to control access to signature operation on behalf of the signatory.

4.2 Assets

The description of each asset provides the type of protection required for each asset ("Protection" part).

Assets are grouped according to whether it is Data created by and for the TOE or Functions provided by the TOE.

4.2.1 Core Group

D.DTBSR

Data to Be Signed Representation received from SCA and transmitted to SERVER as defined in signature activation protocol.

Protection: integrity

D.IDENTIFICATION_DATA_I

These data correspond to Signatory and SCC identification data. These data are used to identify the signatory and SCC and then used as input in SAD computation. These data are supposed to be imported during enrolment phase and stored in the TOE.

Protection: integrity

Application Note:

These data may also optionally be transmitted by SERVER for SAD computation.

These data include a link between identity of signatory and SCC identification mean (also named SCC.ID).

D.SIGNATORY_DATA

These data correspond to link between Signatory and SCD identification data (SCD.ID).

Protection: integrity and confidentiality.

D.SCC_AUTHENTICATION_SecretKey

Secret keys used in symmetric cryptographic functions and private keys used in asymmetric cryptographic functions, used by the TOE for SCC authentication. Key(s) may be generated outside of the TOE and imported in the TOE or generated inside the TOE.

Protection: integrity and confidentiality.

Application Note:

This asset is used by the authentication service running on the TOE. The TOE can contain several Authentication Keys, dedicated to different distant entities.

D.SCC_AUTHENTICATION_PubKey

Public keys (which may be represented as public key certificates) used in asymmetric cryptographic functions, used by the TOE for SCC authentication. Key(s) may be generated outside of the TOE and imported in the TOE or generated inside the TOE.

Protection: integrity.

Application Note:

The public key shall remain consistent with its corresponding private key until it is securely delivered to the CGA.

D.SAP_HSM_AUTHENTICATION_PubKey

Public key used in asymmetric cryptographic functions, used by the TOE for SAP HSM authentication.

Protection: integrity.

D.SAD_KEY

This key is used in SAD computation.

Protection: integrity and confidentiality.

D.SAD

The Signature Activation Data (SAD) are computed by SCC in order to allow access control by SAD HSM to signature operation. It is computed using a cryptographic operation with input D.DTBSR, D.SIGNATORY_DATA, D.SAD_KEY (and D.DTBSR_C when privacy is required).

Protection: integrity and confidentiality.

4.2.1.1 Assets associated to Administrator Role

D.ADMIN_RAD

This asset, associated to the administrator role, corresponds to the reference authentication data used to perform comparison with verification authentication data in Administrator authentication security function.

Protection: integrity and confidentiality.

D.ADMIN_VAD

This asset, associated to the administrator role, corresponds to the verification authentication data generated or imported to be used in Administrator authentication security function. When biometrics is used, the administrator must be involved for the generation of these data.

Protection: integrity and confidentiality.

D.ISSUER_RAD

This asset, associated to the issuer role, corresponds to the reference authentication data used to perform comparison with verification authentication data in issuer authentication security function only available prior operational phase. It shall not be accessed or used during operational phase.

Protection: integrity and confidentiality.

Such assets are also required for Appendix A.

4.2.2 HOLDER-SIDE Authentication Group

See Appendix C.

4.2.3 SERVER-SIDE Authentication Group

See Appendix D.

4.2.4 Privacy Group

See Appendix B.

4.3 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

Assumptions are generic and therefore are associated to CORE group.

A.TSCM_CERTIFIED

It is assumed that the TSCM module is certified according to [PP TSCM]. This module is a part of the TOE remote environment and used for managing signature request (e.g. provide remote TOE authentication and operation for SAP etc.)

A.SAP_HSM_CERTIFIED

It is assumed that the SAP HSM module is certified according to [PP SAP HSM]. This module is a part of the TOE remote environment and used to perform:

- Access control to signature operation based on verification of SAD provided by SCC
- Generation of SCD/SVD key pair
- Request to HSM for signature operation on behalf of signatory performed by the cryptographic module
- Other operations linked to security management

A.PKI

It is assumed that the TOE is used in an environment providing a PKI that generates a certificate for the SCC authentication Private Key. The PKI also manages the validity of Certificates, their end of validity, their possible revocation, in such a way that the TW4S can rely on the Certificate provided by the PKI.

A.ISSUER

It is assumed that the SCC Issuer is trusted and well-trained to follow recommendations for TOE initialization. He possesses the resources required for his tasks and is trained to conduct activities he is responsible for. It is assumed that the SCC Issuer RAD has been securely imported in the pre-personalization phase.

A.ADMINISTRATOR

It is assumed that the SCC administrator is trusted and well-trained to follow recommendations for TOE administration. He possesses the resources required for his tasks and is trained to conduct

activities he is responsible for. Administrator uses its own RAD to be authenticated for administration operations.

A.HOLDER

It is assumed that the Holder of the TOE (i.e., the legitimate device holder) is aware of recommendations for secure usage of TOE and does not disclose his authentication data allowing him to authenticate to the TOE that may lead to voluntary impersonation of the signatory.

A.CERTIF_AUTH

It is assumed that the Certification Authority issuing the certificate for the authentication service and signature service implements practices that conform to an approved certification policy for authentication and signature operation.

When using asymmetric cryptography, it is assumed that the TOE is used in an environment providing a PKI that generates a certificate for the SCC and SAP HSM authentication. The PKI also manages the validity of certificates, their end of validity, their possible revocation, in such a way that the TW4S can rely on the certificate provided by the PKI.

A.KEY_GENERATION

When SCD/SVD key pair and SCC authentication key (Symmetric and/or Asymmetric) are generated outside the TOE, it is assumed that this generation is performed by an authorized person in a way that preserves the integrity and confidentiality of the keys (private and/or symmetric) and integrity of public keys.

The cryptographic keys are supposed to be generated in conformance to the rules and recommendations defined by the relevant Certification Body.

A.EXTERNAL_DATA Protection of Sensitive data outside TOE

Where copies of sensitive data protected by the TOE are managed outside of the TOE, other entities are supposed to provide appropriate protection for copies of that data that may exist outside the TOE.

4.4 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

Application Note is added for each threat to simplify analysis of coverage of authentication threat as defined in [ISO-29115].

Note: Threats are generic and left in Core group when some are specifically associated to a group.

The Attacker role is defined as follows:

Attacker: An attacker is any individual who is attempting to perform actions, which they are not allowed by their access rights as defined in this PP. For such purpose, attacker can try to obtain direct access to TOE (usually under control of signatory) or to access to communication channel between TOE and SERVER without notice of signatory. Such person may have expertise, resources and motivation as expected from an entity with high attack potential.

4.4.1 Enrolment For Authentication

T.SCC_IMPERSONATION_ENR SCC impersonation during enrolment phase

Attacker impersonates using modified or fake SCC during enrolment phase:

- using a genuine SCC with fake or disclosed SCC authentication data,
- using a genuine SCC with disclosed administrator authentication data to modify SCC authentication data,
- using a fake SCC with disclosed authentication data of a genuine SCC to allow fake authentication and retrieving of Administrator or Issuer authentication data.

Threaten Assets: Relevant assets are [D.SCC_AUTHENTICATION_SecretKey, D.SCC_AUTHENTICATION_PubKey, D.ADMIN_RAD, D.ISSUER_RAD].

Such SCC impersonation may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

[ISO-29115] T.Impersonation, T.CredentialCreation:Tampering, T.CredentialCreation:UnauthorizedCreation, T.CredentialIssuance:Disclosure, T.CredentialActivation:Unauthorized Possession, T.CredentialActivation:Unavailability, T.CredentialStorage:Disclosure, T.CredentialStorage:Tampering, T.CredentialStorage:Duplication, T.CredentialStorage:DisclosureByEntity.

T.SERVER_IMPERSONATION_ENR SERVER (SAP HSM) impersonation during enrolment phase

Attacker impersonates using modified or fake SERVER during enrolment phase:

- using a genuine SERVER with fake or disclosed SERVER authentication data,
- using a fake SERVER with disclosed authentication data of a genuine SERVER to allow fake authentication by attacker to SCC.

Threaten Assets: Relevant assets are [D.SAP_HSM_AUTHENTICATION_PubKey].

Such Server impersonation may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

T.SIGNATORY_IMPERSONATION_ENR Signatory impersonation during enrolment phase

Attacker impersonates signatory during enrolment phase:

- by bypassing identity information verification,
- by presenting counterfeited, tampered identity documents without discovery during identity information verification,
- by altering or replacing Signatory identification data during the enrolment process,
- by obtaining a credential that does not belong to him/her and by masquerading as the rightful entity

  that causes the Administrator assess a fake identity to credential allowing fake authentication by attacker to SCC and then to SERVER.

Threaten Assets: Relevant assets are [D.IDENTIFICATION_DATA_I].

Such Signatory impersonation may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

[ISO-29115] T.Impersonation, T.CredentialCreation:UnauthorizedCreation, T.CredentialStorage:Duplication

4.4.2 Enrolment for Signature Function

T.SCC_FORGE_ENR SCC forge during enrolment phase

In the enrolment phase, the attacker modifies inside a genuine SCC, SCD identification data or SAD Key as input for SAD computation in order to obtain a fake SAD. Such a fake SAD may lead to unauthorized signature activation.

Threaten Assets: Relevant assets are [D.SIGNATORY_DATA, D.SAD_KEY].

Such SCC forgery may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

[ISO-29115] T.CredentialCreation: Tampering, T.CredentialCreation: UnauthorizedCreation, T.CredentialStorage: Tampering, T.CredentialStorage: Duplication

4.4.3 Authentication and Secure Channel

T.SCC_IMPERSONATION SCC impersonation in usage phase

Attacker impersonates signatory using a fake SCC during SCC authentication to SERVER using several means as:

- o forging SCC authentication data (SCC key(s), SCC certificate including SCC public key (in the case of use of Asymmetric key pair for SCC authentication)),
- o obtaining SCC authentication data (SCC key(s)) stored in SCC or during its usage,
- o using a weakness in authentication protocol, to allow fake authentication by attacker to SERVER.

Threaten Assets: Relevant assets are [D.SAD_KEY, D.SCC_AUTHENTICATION_SecretKEY, and D.SCC_AUTHENTICATION_PubKey].

Such SCC impersonation may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Note: SAD verification by SAP_HSM confirms usage of SAD_KEY only shared between SCC and SAP_HSM indirectly authenticating SCC and signatory owning SCC. As SAD computation for a given DTBSR is only possible when Signatory is authenticated, SAD verification also confirms authentication of Signatory has been performed in such purpose.

T.SCC_MANINTHEMIDDLE_SERVER Man in Middle between SCC and SERVER

The attacker positions himself between the SCC and the SERVER so that he can intercept and alter the content of the messages (user data and/or data for authentication procotol). The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the SERVER. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other. The attacker tries to gain unauthorized access to the SERVER using method as:

- o Predictable session token,
- o Session Sniffing,
- o Client-side attacks,
- o Man-in-the-middle attack,
- o Man-in-the-browser attack.

By this way, attacker replaces genuine data (DTBSR, SAD or data used to compute SAD) by fake data during transfer between SERVER and SCC leading to unauthorized signature operation activation.

Relevant assets are [D.DTBSR, D.IDENTIFICATION_DATA_I, D.SIGNATORY_DATA, D.SAD].

Such man in the middle attack may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

[ISO-29115] T.ManInTheMiddle

T.SCC_AUTHENTICATION_PHISHING Forge SCC by Phishing

Attacker forges SCC authentication by masquerading legitimate SERVER using phishing method to obtain authentication from valid SCC allowing forged authentication from an invalid SCC.

Threaten Assets: Relevant assets are [D.DTBSR].

Such SCC impersonation by phishing may contribute to bypass signature activation protocol that may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

[ISO-29115] T.Phishing

T.SAD_FORGERY Signature Activation Data Forgery

Attacker forges SAD during transfer between SCC and SERVER leading to generation of valid SAD with forged DTBS/R.

Threaten Assets: Relevant assets are [D.SAD].

Such SAD forgery may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

SAD computed using a strong cryptographic function may be not subject to such issue as SAD verification works only if SAD has not been forged.

4.4.4 SAD Computation

Fake SAD computation or replay of SAD computation may lead to potential threat in signature activation protocol violating access control to signature operation done by SAP HSM.

T.UNAUTHORIZED_SIGNATURE_ACTIVATION Unauthorized signature operation activation

An attacker bypasses one or several steps of signature activation protocol allowing unauthorized signature activation on SAP HSM by:

- forging SAD during its computation (implying or not forged SADKey)
- generating valid SAD with forged DTBS/R or forged link with SCD or signatory identity,
- generating valid SAD without Signatory consent or Signatory authentication

Threaten Assets: Relevant assets are [D.IDENTIFICATION_DATA_I, D.SIGNATORY_DATA, D.DTBSR, D.SAD_KEY, D.SAD].

Such bypass of steps of signature activation protocol may lead to unauthorized signature operation on behalf of signatory in the SERVER.

Application Note:

SAD computation is associated to DTBS/R, link with SCD.ID and Signatory ID.

T.REPLAY_SIGNATURE_ACTIVATION Signature activation replay

An attacker illegitimately replays steps of signature activation protocol allowing unauthorized signature activation on SAP HSM.

Threaten Assets: Relevant assets are [D.SAD].

Such replay of steps of signature activation protocol may lead to unauthorized signature operation on behalf of signatory in the SERVER.

4.4.5 Administration

Threats associated to unauthorized administration operations on SCC may lead to insecure usage of SCC are defined in Appendix A.

4.4.6 Platform Environment

The following Threats rely on the underlying platform and are therefore an environmental issue.

T.ABUSE-INIT_FUNC Abuse of Enrolment Functions in Operational phase

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization, personalization and enrolment in the operational phase after delivery to the TOE. Threatened assets: confidentiality of User Data and TSF-data of the TOE

Threatened assets: Threaten Assets: Relevant assets are [ALL] according to configuration including, integrity and authenticity of the TOE, availability of the functionality of the TOE.

Application Note:

This generic threat is more specifically seen in T.SCC_FORGE_ENR.

T.INFORMATION_LEAKAGE Information Leakage from platform

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the platform or/and exchanged between the TOE on the platform and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Threatened assets: confidentiality of User Data and TSF-data of the TOE including [D.SCC_AUTHENTICATION_SecretKey, D.SAD_KEY, and D.SAD] according to configuration.

Application note: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements

T.PHYS-TAMPER Physical Tampering

An attacker may perform physical probing of the TOE in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the TOE in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the TOE. Threatened assets: integrity and authenticity of the TOE, availability of the functionality of the TOE, confidentiality of User Data and TSF-data of the TOE.

Threatened assets: Threaten Assets: Relevant assets are [ALL] according to configuration including, integrity and authenticity of the TOE, availability of the functionality of the TOE.

Application Note: [ISO-29115] T.Impersonation, T.CredentialStorage:Disclosure, T.CredentialStorage:Tampering, T.CredentialStorage:Duplication.

Physical tampering may be focused directly on the disclosure or manipulation of the user data or indirectly by preparation of the TOE with permanent or temporary modification of associated security features.

T.MALFUNCTION Malfunction due to Environmental Stress

An attacker may cause a malfunction the TOE hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the TOE outside the normal operating conditions, exploiting errors in the TOE's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threatened assets: Relevant assets are [ALL] according to configuration including, integrity and authenticity of the TOE, availability of the functionality of the TOE.

Application Note:

A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface.

4.4.7 Threats and Associated Assets

The following table summarizes links between threats and associated assets.

	Sec Property	***Enrolment For Authentication***	T.SIGNATORY_IMPERSONATION_ENR	T.SCC_IMPERSONATION_ENR	T.SERVER_IMPERSONATION_ENR	***Enrolment For Signature Function***	T.SCC_FORGE_ENR SCC	***Authentication And Secure Channel***	T.SCC_IMPERSONATION	T.SCC_MANINTHEMIDDLE_SERVER	T.SCC_AUTHENTICATION_PHISHING	T.SAD_FORGERY
D.DTBSR	**I**									X	X	
D.IDENTIFICATION_DATA_I	**I**		X							X		
D.SIGNATORY_DATA	**IC**						X					
D.ADMIN_RAD	**IC**			X								
D.ADMIN_VAD	**IC**											
D.ISSUER_RAD	**IC**			X								
D.SCC_AUTHENTICATION_SecretKey	**IC**			X					X			
D.SCC_AUTHENTICATION_PubKey	**I**			X					X			
D.SAP_HSM_AUTHENTICATION_PubKey	**I**				X							
D.SAD_KEY	**IC**						X					
D.SAD	**IC**											X

Table 2 - Threats and associated Assets (1/2)

	SAD Computation	T.UNAUTHORIZED_SIGNATURE_ACTIVATION	T.REPLAY_SIGNATURE_ACTIVATION	***Platform Environment***	T.ABUSE-INIT_FUNC	T.INFORMATION_LEAKAGE	T.PHYS-TAMPER	T.MALFUNCTION
D.DTBSR		X			X		X	X
D.IDENTIFICATION_DATA_I		X			X	X	X	X
D.SIGNATORY_DATA		X			X	X	X	X
D.ADMIN_RAD					X	X	X	X
D.ADMIN_VAD					X	X	X	X
D.ISSUER_RAD					X	X	X	X
D.SCC_AUTHENTICATION_SecretKey					X	X	X	X
D.SCC_AUTHENTICATION_PubKey					X		X	X
D.SSP_HSM_AUTHENTICATION_PubKey					X		X	X
D.SAD_KEY		X			X	X	X	X
D.SAD		X	X		X	X	X	X

Table 3 - Threats and associated Assets (2/2)

4.5 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 (see CC part 1, sec. 3.2).

OSP are generic and therefore are associated to CORE group.

OSP.ENROLMENT_RULES

The Holder enrolment is done using the rules conformant for LoA4 level as defined in [ISO-29115] including a secure identity proofing policy and procedure.

OSP.ENROLMENT_SECURE_PROCESS

Enrolment and credential management process shall be done securely according to rules conformant for LoA4 level as defined in [ISO-29115]. It includes a secure process for credential creation, issuance, storage, revocation, destruction and renewal. A record of the registration, history, and status of each credential (including revocation) shall be maintained by the CSP. The duration of retention shall be specified in the CSP policy.

OSP.SECURE_USEOFCREDENTIAL

Use of credentials for Authentication shall be done securely:

- Two or more credentials implementing different authentication factors shall be used to be conformant with LOA defined in [ISO-29115],
- Specific security features shall be used to deter brute force and rainbow table attacks,
- If authentication exchange over a network is used, the data shall be properly protected prior to transfer to keep data confidentiality,
- If biometry is used, liveness detection techniques shall be used to identify the use of artificial biometric characteristics.

OSP.CRYPTO Use of approved cryptographic algorithms

The TOE shall provide cryptographic functions that are endorsed by recognized authorities as appropriate for use by TSPs.

5 Security Objectives

5.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

5.1.1 Enrolment For Authentication

The following objectives are associated to authentication elements managed during enrolment.

OT.AUTHENTICATION_KEY_IMPORT AUTH Key Import

The TOE shall be able to securely import authentication key (Symmetric and/or Asymmetric). The import of the key is only allowed:

- during the personalization phase, when the Issuer is authenticated,
- during the enrolment phase, when the Administrator is authenticated. The import of the key shall be protected against disclosure and/or modification.

OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation

The TOE shall be able to generate SCC authentication keys and export public key (in the case of use of Asymmetric Key pair for SCC authentication) to request generation of SCC authentication certificate. The generation of the key is only allowed:

- during the personalization phase, when the Issuer is authenticated,
- during the enrolment phase, when the Administrator is authenticated.

When a new SCC authentication key is generated, any previous SCC authentication key shall be deleted.

OT.SIGNATORY_IDDATA_ENR Signatory Identification data Importation during Enrolment phase

The TOE shall be able to securely import the Signatory identification data during enrolment phase when the Administrator is authenticated.

5.1.2 Enrolment For Signature Function

The following objectives are associated to signature elements managed during enrolment.

OT.SCD_ID_IMPORT SCD Identification Data Import

The TOE shall be able to securely (confidentiality and integrity protection) import SCD Identification data.

OT.SAD_KEY_IMPORT SAD KEY Import

The TOE shall be able to securely (confidentiality and integrity protection) import SAD KEY.

5.1.3 Authentication and Secure Channel

The following objectives are associated to authentication and secure channel management during operational phase.

OT.SCC_AUTHENTICATION SCC Authentication data for SERVER (TSCM or SAP HSM)

The TOE shall provide information to SERVER to be authenticated (on behalf of the Holder) by the SERVER. This authentication shall implement a Symmetric and/or Asymmetric cryptographic protocol. The authentication of the TOE must be performed only if SERVER authentication by the TOE has been already done.

OT.SERVER_AUTHENTICATION SERVER Authentication by TOE

The TOE shall provide mechanisms to authenticate the SERVER on SERVER request. Before the TOE authenticates the SERVER, the TOE shall not deliver data to SERVER that could enable the TOE identification.

OT.SECURE_CHANNEL Secure channel between SERVER and TOE

The TOE shall provide mechanisms to answer to creation request of a secure channel between TOE and SERVER and to manage exchange in the secure channel to assure integrity of all data exchange and confidentiality of specific data exchange (as SAD and optional VAD_SERVER-SIDE) in the secure channel.

5.1.4 SAD Computation

The following objectives are associated to SAD computation performed during operational phase.

OT.SIGN_ACTIVATION_PROTECTION Access Control to SAD Computation

The TOE shall provide features to protect against sending to SERVER any unauthorized signature request. Such protection is based on a signature activation protocol where execution flow control avoids any bypass of security operations (holder, SERVER authentication, SCC authentication and SAD computation, Signature request transfer).

OT.DTBSR_SAD_INTEGRITY DTBSR and SAD Integrity

The TOE shall provide mechanisms to manage integrity of SAD and relevant data during SAD computation and transmission to SERVER.

OT.SAD_COMPUTATION SAD Computation For Signature Operation Anti Replay

The TOE shall provide mechanisms to protect against replay of valid signature request by computing unique SAD for each signature request using D.SADKey and inputs as dedicated DTBSR, link with SCD and signatory identity.

5.1.5 Protection of the TSF

The following objectives are associated to protection of TSF using platform security features during all phases.

OT.PROTECTION Sensitive Data Protection

The TOE shall be able to protect any sensitive data, Assets and TSF data, against unauthorized disclosure and/or modification. This protection applies when the data are on the TOE.

5.1.6 Cryptography

The following objectives are associated to cryptographic operations performed during operational phase.

OT.CRYPTO Cryptographic Operations

The TOE shall implement cryptographic functions in accordance with the rules and recommendations defined by the Certification Body.

5.2 Security Objectives for the Operational Environment

This section describes the security objectives for the environment of the TOE addressing the aspects of identified threats, organizational security policies and assumptions.

5.2.1 SCC Developement Phase

5.2.1.1 Platform Environment

The following platform security objectives address the aspects of identified threats to be countered involving TOE's environment on platform.

Since the TOE of the ST includes the Platform which belongs to the operational environment of the TOE of the PP, all the security objectives on the Platform introduced in this PP shall be redefined as security objectives “on the TOE” in the ST.

OE.PROT_ABUSE_FUNC Protection against Abuse of Functionality

The Platform must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OE.PROT_INF_LEAK Protection against Information Leakage

The Platform must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the SCC

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the Platform and/or
- by a physical manipulation of the Platform.

Application Note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the platform or operations enforced by an attacker.

OE.PROT_PHYS-TAMPER Protection against Physical Tampering

The Platform must be tamper resistant with accurate detection and reaction to actually prevent an attacker from extracting or altering security data or security feature and providing protection of confidentiality and integrity of the User Data, the TSF-data and the TOE Embedded Software.

OE.PROT_MALFUNCTION Protection against Malfunctions

The Platform must ensure its correct operation. The Platform must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

OE.CRYPTO Development of Cryptography according CB rules

The Platform shall provide cryptographic functions in accordance with the rules and recommendations defined by the Certification Body.

5.2.2 SCC Enrolment Phase

OE.TRUSTED_PERSO_ENROLMENT Trusted Environment and Tools during personalization and enrolment phase

The TOE relies on its environment and secure tools to protect integrity and confidentiality of the sensitive data during personalization and enrolment operations, as the following but not limited to:

- keys and sensitive data generation, distribution and storage, associated to administrator authentication,
- keys and sensitive data generation, distribution and storage, associated to holder, SERVER authentication or SCC authentication,
- certificate generation request and distribution,
- keys and sensitive data generation, distribution and storage associated to signature activation protocol.

OE.ISSUER Trusted and Trained Issuer

The Issuer shall possess the skills and resources required for his tasks and is trained to conduct activities he is responsible for. It is responsible

5.2.3 SCC Operational Phase

OE.HOLDER Responsible Holder

The Holder of the SCC (i.e., the legitimate device holder) shall not share or disclose his authentication data to avoid any impersonation. The Holder shall keep control on its SCC to avoid inconsistent activation of signature operation on its behalf.

OE.ADMINISTRATOR Trusted and Trained Administrator

The Administrator shall possess the skills and resources required for his tasks and is trained to conduct activities he is responsible for.

5.2.4 TW4S Environment

OE.TRUSTED_TW4S TW4S as a Trusted Environment in operational phase

TW4S must include TSCM certified according to [PP TSCM] and SAP HSM certified according to [PP SAP HSM]. TW4S is authenticated by SCC to be trusted and gives confidence that it manages securely sensitive data exchange and sensitive operations. In operational phase, it manages securely at least SCC authentication, SERVER authentication, data exchange relevant for authentication and signature operation in secure channel and signature activation protocol.

OE.AUTH_CERTIF_VERIF SCC Certificate Verification

The SERVER shall verify the validity of the SCC certificate (in the case of use of Asymmetric Key pair for SCC authentication) before considering the SCC as authenticated on behalf of holder and granting to the service. The certificate verification shall include in particular:

- the verification that the current date belongs to the validity period of the certificate,
- the verification that the certificate has not been revoked.

OE.CERTIF_AUTH

The Certification Authority issuing the certificate for the authentication service and signature service shall implements practices that conform to an approved certification policy for authentication and signature operation.

When using asymmetric cryptography, the TOE shall be used in an environment providing a PKI that generates a certificate for the SCC authentication Private Key. The PKI also manages the validity of Certificates, their end of validity, their possible revocation, in such a way that the TW4S can rely on the Certificate provided by the PKI.

OE.SECURE_COPY Management of Sensitive Data in operational phase

The confidential sensitive data, Assets and TSF data, managed inside the TOE shall not be compromised in operational phase by copies of such data that may exist outside the TOE.

OE.KEY_GENERATION Secure Key Generation

When keys are not generated by the TOE, the device generating the key shall ensure the integrity and the confidentiality of Private Key (Asymmetric key pair for SCC authentication) and/or Symmetric Key and the integrity of the Public key (Asymmetric key pair for SCC authentication) until it is transferred to the CA, protected in integrity.

5.3 Security Objectives Rationale

5.3.1 SPD and Security Objectives

The following tables provide mapping of security problem definition to objectives.

Then a rationale is provided to explain how each Threat, OSP and Assumptions are covered by objectives.

	Enrolment For Authentication	OT.AUTHENTICATION_KEY_IMPORT	OT.AUTHENTICATION_KEY_GENERATE	OT.SIGNATORY_IDDATA_ENR	***Enrolment For Signature Function***	OT.SCD_ID_IMPORT	OT.SAD_KEY_IMPORT	***Authentication And Secure Channel***	OT.SCC_AUTHENTICATION	OT.SERVER_AUTHENTICATION	OT.SECURE_CHANNEL
Enrolment For Authentication											
T.SIGNATORY_IMPERSONATION_ENR				X							
T.SCC_IMPERSONATION_ENR		X	X								
T.SERVER_IMPERSONATION_ENR		X									
Enrolment For Signature Function											
T.SCC_FORGE_ENR						X	X				
Authentication And Secure Channel											
T.SCC_IMPERSONATION									X		
T.SCC_MANINTHEMIDDLE_SERVER									X	X	X
T.SCC_AUTHENTICATION_PHISHING										X	
T.SAD_FORGERY											X
SAD Computation											
T.UNAUTHORIZED_SIGNATURE_ACTIVATION											
T.REPLAY_SIGNATURE_ACTIVATION											
Platform Environment											
T.ABUSE-INIT_FUNC											
T.INFORMATION_LEAKAGE											
T.PHYS-TAMPER											
T.MALFUNCTION											

Table 4 - Threats and TOE Security Objectives - Coverage (1/2)

	SAD Computation	OT.SIGN_ACTIVATION_PROTECTION	OT.DTBSR_SAD_INTEGRITY	OT.SAD_COMPUTATION	***Protection of the TSF***	OT.PROTECTION	***Cryptography***	OT.CRYPTO
Enrolment For Authentication								
T.SIGNATORY_IMPERSONATION_ENR						X		
T.SCC_IMPERSONATION_ENR						X		
T.SERVER_IMPERSONATION_ENR						X		
Enrolment For Signature Function								
T.SCC_FORGE_ENR						X		
Authentication And Secure Channel								
T.SCC_IMPERSONATION						X		X
T.SCC_MANINTHEMIDDLE_SERVER						X		X
T.SCC_AUTHENTICATION_PHISHING						X		X
T.SAD_FORGERY						X		X
SAD Computation								
T.UNAUTHORIZED_SIGNATURE_ACTIVATION		X	X	X		X		X
T.REPLAY_SIGNATURE_ACTIVATION		X		X		X		X
Platform Environment								
T.ABUSE-INIT_FUNC						X		
T.INFORMATION_LEAKAGE						X		X
T.PHYS-TAMPER						X		
T.MALFUNCTION						X		

Table 5 - Threats and TOE Security Objectives - Coverage (2/2)

	Enrolment For Authentication	OT.AUTHENTICATION_KEY_IMPORT	OT.AUTHENTICATION_KEY_GENERATE	OT.SIGNATORY_IDDATA_ENR	***Enrolment For Signature Function***	OT.SCD_ID_IMPORT	OT.SAD_KEY_IMPORT	***Authentication And Secure Channel***	OT.SCC_AUTHENTICATION	OT.SERVER_AUTHENTICATION	***Authentication And Secure Channel***	OT.SECURE_CHANNEL
OSP.AUTHENTICATION_PROTOCOL									X	X		X
OSP.ENROLMENT_RULES		X	X	X		X	X					
OSP.ENROLMENT_SECURE_PROCESS		X	X	X		X	X					
OSP.SECURE_USEOFCREDENTIAL												X
OSP.CRYPTO												

Table 6 - OSP and TOE Security Objectives - Coverage (1/2)

	SAD Computation	OT.SIGN_ACTIVATION_PROTECTION	OT.DTBSR_SAD_INTEGRITY	OT.SAD_COMPUTATION	***Protection of the TSF***	OT.PROTECTION	***Cryptography***	OT.CRYPTO
OSP.AUTHENTICATION_PROTOCOL								
OSP.ENROLMENT_RULES								
OSP.ENROLMENT_SECURE_PROCESS								
OSP.SECURE_USEOFCREDENTIAL								
OSP.CRYPTO								X

Table 7 - OSP and TOE Security Objectives - Coverage (2/2)

	Platform Environment	OE.PROT_ABUSE_FUNC	OE.PROT_INF_LEAK	OE.PROT_PHYS-TAMPER	OE.PROT_MALFUNCTION	OE.CRYPTO	***Enrolment Phase***	OE.TRUSTED_PERSO_ENROLMENT	OE.ISSUER	***Operational Phase***	OE.HOLDER	OE.ADMINISTRATOR	OE.TRUSTED_TW4S	OE.AUTH_CERTIF_VERIF	OE.CERTIF_AUTH	OE.SECURE_COPY	OE.KEY_GENERATION
Enrolment For Authentication																	
T.SIGNATORY_IMPERSONATION_ENR								X	X							X	
T.SCC_IMPERSONATION_ENR								X	X							X	X
T.SERVER_IMPERSONATION_ENR								X	X							X	
Enrolment For Signature Function																	
T.SCC_FORGE_ENR								X	X							X	X
Authentication And Secure Channel																	
T.SCC_IMPERSONATION													X	X		X	
T.SCC_MANINTHEMIDDLE_SERVER						X							X	X			
T.SCC_AUTHENTICATION_PHISHING													X				
T.SAD_FORGERY																	
SAD Computation																	
T.UNAUTHORIZED_SIGNATURE_ACTIVATION						X					X						
T.REPLAY_SIGNATURE_ACTIVATION						X											
Platform Environment																	
T.ABUSE-INIT_FUNC		X															
T.INFORMATION_LEAKAGE			X														
T.PHYS-TAMPER				X													
T.MALFUNCTION					X												

Table 8 - Threats and Security Objectives for Environment - Coverage

	SCC Development Phase	OE.PROT_ABUSE_FUNC	OE.PROT_INF_LEAK	OE.PROT_PHYS-TAMPER	OE.PROT_MALFUNCTION	OE.CRYPTO	***SCC Enrolment Phase***	OE.TRUSTED_PERSO_ENROLMENT	OE.ISSUER	***SCC Operational Phase***	OE.HOLDER	OE.ADMINISTRATOR	***TW4S Environment***	OE.TRUSTED_TW4S	OE.AUTH_CERTIF_VERIF	OE.CERTIF_AUTH	OE.SECURE_COPY	OE.KEY_GENERATION
OSP.AUTHENTICATION_PROTOCOL						X								X				
OSP.ENROLMENT_RULES								X	X									
OSP.ENROLMENT_SECURE_PROCESS								X	X									X
OSP.SECURE_USEOFCREDENTIAL											X							
OSP.CRYPTO						X												
A.ISSUER									X									
A.ADMINISTRATOR												X						
A.HOLDER											X							
A.CERTIF_AUTH																X		
A.KEY_GENERATION																		X
A.EXTERNAL_DATA																	X	
A.TSCM_CERTIFIED														X				
A.SAP_HSM_CERTIFIED														X				
A.PKI															X			

Table 9 - OSP, Assumptions and Security Objectives for the Operational Environment - Coverage

The following paragraphs provide a rationale for enforcement of threats by the security objectives.

Enrolment For Authentication

T.SIGNATORY_IMPERSONATION_ENR is countered by **OT.SIGNATORY_IDDATA_ENR** assuming secure import of the Signatory Identification data during enrolment phase. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGNATORY_IMPERSONATION_ENR is also countered by **OE.TRUSTED_PERSO_ENROLMENT** providing a trusted environment for personalization and enrolment, **OE.ISSUER** assuming that issuer is trusted and well-trained and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

T.SCC_IMPERSONATION_ENR is countered by **OT.AUTHENTICATION_KEY_IMPORT** assuming secure import of the SCC and SERVER authentication keys and

OT.AUTHENTICATION_KEY_GENERATE assuming secure generation of the SCC authentication keys.

T.SCC_IMPERSONATION_ENR is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SCC_IMPERSONATION_ENR is also countered by **OE.TRUSTED_PERSO_ENROLMENT** providing a trusted environment for personalization and enrolment, **OE.ISSUER** assuming that issuer is trusted and well-trained, **OE.KEY_GENERATION** assuming secure key generation and management and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

T.SERVER_IMPERSONATION_ENR is countered by **OT.AUTHENTICATION_KEY_IMPORT** assuming secure import of the SERVER authentication keys.

T.SERVER_IMPERSONATION_ENR is countered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SERVER_IMPERSONATION_ENR is also countered by **OE.TRUSTED_PERSO_ENROLMENT** providing a trusted environment for personalization and enrolment, **OE.ISSUER** assuming that issuer is trusted and well-trained and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

Enrolment For Signature Function

T.SCC_FORGE_ENR is countered by OT.SCD_ID_IMPORT assuming secure import of the SCD Identification data and **OT.SAD_KEY_IMPORT** assuming secure import of SAD key**.** It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SCC_FORGE_ENR is also countered by **OE.TRUSTED_PERSO_ENROLMENT** providing a trusted environment for personalization and enrolment, **OE.ISSUER** assuming that issuer is trusted and well-trained, **OE.KEY_GENERATION** assuming secure key generation and management and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

Authentication And Secure Channel

T.SCC_IMPERSONATION is countered by **OT.SCC_AUTHENTICATION** providing information to SERVER to authenticate SCC. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SCC_IMPERSONATION is also countered by **OE.TRUSTED_TW4S** requiring authentication between items included in TW4S, **OE.AUTH_CERTIF_VERIF** managing validity of SCC certificate for authentication and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

T.SCC_MANINTHEMIDDLE_SERVER is countered by **OT.SCC_AUTHENTICATION** providing information to SERVER to authenticate SCC and **OT.SERVER_AUTHENTICATION** requiring SERVER to be authenticated. It is also covered by **OT.SECURE_CHANNEL** requiring a secure channel to avoid data manipulation during transfer and by **OT.PROTECTION** and **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

T.SCC_MANINTHEMIDDLE_SERVER is also countered by **OE.TRUSTED_TW4S** requiring authentication between items included in TW4S, **OE.AUTH_CERTIF_VERIF** managing validity of SCC certificate for authentication and countered by **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure.

T.SCC_AUTHENTICATION_PHISHING is countered by **OT.SERVER_AUTHENTICATION** requiring SERVER to be authenticated.

T.SCC_AUTHENTICATION_PHISHING is also countered by **OE.TRUSTED_TW4S** requiring authentication between items included in TW4S.

T.SAD_FORGERY is countered by **OT.SECURE_CHANNEL** requiring a secure channel to avoid data manipulation during transfer. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification and by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

SAD Computation

T.UNAUTHORIZED_SIGNATURE_ACTIVATION is countered by **OT.SIGN_ACTIVATION_PROTECTION** avoiding any bypass of SAP, **OT.DTBSR_SAD_INTEGRITY** managing SAD integrity and **OT.SAD_COMPUTATION** generating unique SAD avoiding replay of signature operation. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification and by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

T.UNAUTHORIZED_SIGNATURE_ACTIVATION is also countered by **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure and **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data.

T.REPLAY_SIGNATURE_ACTIVATION is countered by **OT.SIGN_ACTIVATION_PROTECTION** avoiding any bypass of SAP and **OT.SAD_COMPUTATION** generating unique SAD avoiding replay of signature operation.

It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification and by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

T.REPLAY_SIGNATURE_ACTIVATION is also countered by **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure.

Platform Environment

The following Threats rely on the underlying platform and are therefore an environmental issue.

T.ABUSE-INIT_FUNC is countered by platform security objectives as **OE.PROT_ABUSE_FUNC** but it is also partially covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.INFORMATION_LEAKAGE is countered by platform security objectives as **OE.PROT_INF_LEAK** but it is also partially covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification and by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

T.PHYS-TAMPER is countered by platform security objective as **OE.PROT_PHYS-TAMPER.**

T.MALFUNCTION is countered by platform security objectives as **OE.PROT_MALFUNCTION** but it is also partially covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

The following paragraphs provide a rationale for enforcement of OSP by the security objectives.

OSP.ENROLMENT_RULES is covered by **OT.AUTHENTICATION_KEY_IMPORT** assuming secure import of the SCC and SERVER authentication keys, **OT.AUTHENTICATION_KEY_GENERATE** assuming secure generation of the SCC authentication keys. It is also covered by **OT_SIGNATORY_IDDATA_ENR** assuming secure import of the Signatory identification data, **OT.SCD_ID_IMPORT** assuming secure import of the SCD Identification data and **OT.SAD_KEY_IMPORT** assuming secure import of SAD key.

OSP.ENROLMENT_RULES is also covered by **OE.TRUSTED_PERSO_ENROLMENT** providing a trusted environment for personalization and enrolment and **OE.ISSUER** assuming that issuer is trusted and well-trained.

OSP.ENROLMENT_SECURE_PROCESS is covered by **OT.AUTHENTICATION_KEY_IMPORT** assuming secure import of the SCC and SERVER authentication keys, **OT.AUTHENTICATION_KEY_GENERATE** assuming secure generation of the SCC authentication keys during the enrolment phase. It is also covered by **OT_SIGNATORY_IDDATA_ENR** assuming secure import of the Signatory identification data, **OT.SCD_ID_IMPORT** assuming secure import of the SCD Identification data and **OT.SAD_KEY_IMPORT** assuming secure import of SAD key.

OSP.ENROLMENT_SECURE_PROCESS is covered by **OE.TRUSTED_PERSO_ENROLMENT** providing secure practices for personalization and enrolment and **OE.ISSUER** assuming that issuer is trusted and well-trained for administration tasks.

OSP.SECURE_USEOFCREDENTIAL is covered by **OT.SECURE_CHANNEL** requiring a secure channel to avoid data disclosure during transfer (if any).

OSP.SECURE_USEOFCREDENTIAL is also covered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data.

OSP.CRYPTO is also covered by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure and **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure.

The following paragraphs provide a rationale for coverage of Assumptions by security objectives.

A.TSCM_CERTIFIED is covered by **OE.TRUSTED_TW4S** requiring certification of TSCM.

A.SAP_HSM_CERTIFIED is covered by **OE.TRUSTED_TW4S** requiring certification of SAP HSM.

A.PKI is covered by **OE.AUTH_CERTIF_VERIF** managing validity of SCC certificate for authentication.

A.ISSUER is covered by **OE.ISSUER** assuming that issuer is trusted and well-trained.

A.ADMINISTRATOR is covered by **OE.ADMINISTRATOR** assuming that administrator is trusted and well-trained.

A.HOLDER is covered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data.

A.CERTIF_AUTH is covered by **OE.CERTIF_AUTH** implementing practices that conform to an approved certification policy for authentication and signature operation and providing a PKI that generates a certificate for the SCC authentication Private Key (When using asymmetric cryptography).

A.KEY_GENERATION is covered by **OE.KEY_GENERATION** assuming secure key generation and management.

A.EXTERNAL_DATA is covered by **OE.SECURE_COPY** assuming secure management of sensitive data external to TOE in operational phase.

6 Extended Requirements

This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [PP BSI-0084], other components are defined in this protection profile.

6.1 Extended Families

6.1.1 Extended Family FIA_API - Authentication Proof of Identity

6.1.1.1 Description

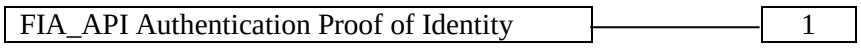
To describe the IT security functional requirements of the TOE a functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [CC3], chapter "Extended components definition (APE_ECD)") from a TOE point of view.

Family Behaviour

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:



FIA_API.1 Authentication Proof of Identity, provides proof of the identity of the TOE, an object or an authorized user or role to an external entity.

Management	FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	FIA_API.1 There are no actions defined to be auditable.

6.1.1.2 Extended Components

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [selection: TOE, [assignment: object, authorized user or role]] to an external entity.

6.1.2 Extended Family FDP_SDC - Stored data confidentiality

1 To describe the IT security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here

2 The family "Stored data confidentiality (FDP_SDC)" is specified as follows.

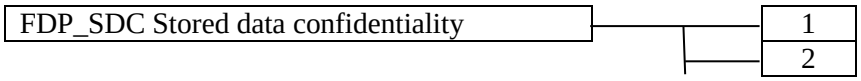
3 The other families of the Class FDP do not describe confidentiality of stored data by the TOE. The following paragraph defines the family FDP_SDC in the style of the Common Criteria part 2 (cf. [3], chapter "Extended components definition (APE_ECD)") from a TOE point of view.

4 FDP_SDC Stored data confidentiality [1]

Family Behaviour

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling:



FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management FDP_SDC.1
There are no management activities foreseen.

Audit: FDP_SDC.1
There are no actions defined to be auditable.

[1] Component initially created in [PP0084]

6.1.2.1 Extended Components

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area].

FDP_SDC.2 Requires the TOE to protect the confidentiality of information of the user data for a specified type of user data.

Management FDP_SDC.2
There are no management activities foreseen.

Audit: FDP_SDC.2
There are no actions defined to be auditable.

FDP_SDC.2 Stored data confidentiality by type

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.2.1 The TSF shall ensure the confidentiality of the information of the user data according to [assignment: *data type*] while it is stored in the TOE.

7 Security Requirements

7.1 Security Functional Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 of the CC [CC1]. Each of these operations is used in this PP.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections to be filled in by the ST author appear in square brackets in bold text with an indication that a selection is to be made, [selection:], and are italicized.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments to be filled in by the ST author appear in square brackets in bold text with an indication that an assignment is to be made [assignment:], and are italicized.

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

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

7.1.1 Subjects, Objects and Security Attributes

The following tables are given as example for TSP. ST writer may use it or decide to extend it.

TOE may works with the subjects (prefixed with an "S") and associated roles defined in the following table:

Subject	Role
S.Issuer	It acts for TOE personalization purpose on behalf of Issuer during personalization phase.
S.Administrator	It acts for TOE administration purpose on behalf of administrator during enrolment.
S.User	It acts for any operations allowed prior identification and authentication during usage phase.
S.Signatory	It acts for usage purpose on behalf of Signatory (authenticated) during usage phase.
S.Command_manager	It manages commands sent to the TOE and corresponding responses from the TOE, including import/export of sensitive assets.
S.Communication_manager	It provides secure communication service between TOE and SERVER (TSCM or SAP HSM).

Table 10 - Subjects and Roles

Application note: SCC is supposed to be under control of signatory, therefore user is supposed to be identical to signatory. But only signatory authentication gives evidence about this assumption.

The TOE behavior is controlled using security attributes (prefixed with an "AT") defined in the following table:

Subject	Security attribute	Possible Values	Initial Values
S.Command_manager	AT.Phase	Enrolment, Usage, Blocked	Perso
S.Command_manager	AT.SecureState	Secure, Unsecure	Secure
S.Command_manager	AT.Authenticated_user	Issuer, Administrator, Signatory, User	None
S.Command_manager	AT.Access_Control	Authorized, not authorized	Not authorized
S.Communication_manager	AT.SecureChannel	InProgress, Open, None	None
S.Issuer	AT.Authenticated_user	Issuer	None
S.Issuer	AT.ISS_RAD_retry_counter	0 to ISSUER_MAX_RETRY_COUNTER	0
S.Administrator	AT.Authenticated_user	Administrator	None
S.Administrator	AT.ADMIN_RAD_retry_counter	0 to ADMINISTRATOR_MAX_RETRY_COUNTER	0
S.Administrator	AT.RADType	HOLDER-SIDE, SERVER-SIDE	HOLDER-SIDE
S.Signatory	AT.Authenticated_user	Signatory	None, Signatory
S.Signatory	AT.RAD_Value	Arbitrary value	Null
S.Signatory	AT.SIG_RAD_retry_counter	0 to SIGNATORY_MAX_RETRY_COUNTER	0
S.User	AT.Authenticated_user	User	None

Table 11 - Subjects and Security Attributes

The previous table describes how a security attribute can be modified by a subject from an initial value to other possible values.

List of operations per subjects and per phase are defined in the following table:

Subject	**Operations**	**Objects**	**Comments / Phase**
S.Command_manager	EXECUTE, ACCESS	All authorized commands	If commands are authorized in current phase [all phases]
S.Communication_manager	CREATE, MANAGE, COMPUTE	Manage all authorized commands requiring Secure Channel Manage the signature request received from SCA and transmitted to SERVER Compute data for authentication by SERVER Create and manage exchanges in secure channel between TOE and SERVER	Authorize exchange when secure channel is setup. [all phases]
S.Issuer	Authenticate as Issuer	ISSUER_VAD	Personalization (*)
S.Issuer	CHANGE PHASE	PHASE	Personalizati

Subject	Operations	Objects	Comments / Phase
			on (*)
S.Issuer	WRITE, STORE, IMPORT	IDENTIFICATION_DATA	Personalization (*)
S.Issuer	STORE, IMPORT	ADMIN_RAD	Personalization (*)
S.Issuer	STORE, IMPORT	ISSUER_RAD	Personalization (*)
S.Issuer	IMPORT, GENERATE	SCC_AUTHENTICATION_SECRET_KEY	Personalization (*)
S.Issuer	IMPORT, GENERATE, EXPORT	SCC_AUTHENTICATION_PUB_KEY	Personalization (*)
S.Issuer	Change RadType	RADType	Personalization (*)
S.Administrator	Authenticate as Administrator	ADMIN_RAD	Enrolment phase
S.Administrator	IMPORT, GENERATE, ACTIVATE, DEACTIVATE, DESTRUCT	SCC_AUTHENTICATION_SECRET_KEY	Enrolment phase
S.Administrator	IMPORT, GENERATE, EXPORT	SCC_AUTHENTICATION_PUB_KEY	Enrolment phase
S.Administrator	IMPORT	SAP_HSM_AUTHENTICATION_PUB_KEY	Enrolment phase
S.Administrator	IMPORT	TSCM_AUTHENTICATION_PUB_KEY	Enrolment phase
S.Administrator	STORE, IMPORT	SAD_KEY	Enrolment phase
S.Administrator	STORE, IMPORT, ACTIVATE, DEACTIVATE	SIGNATORY_RAD	Enrolment phase
S.Administrator	Change Phase	PHASE	Enrolment phase
S.Administrator	WRITE, STORE, IMPORT	IDENTIFICATION_DATA_I	Enrolment phase
S.Administrator	IMPORT	SIGNATORY_DATA	Enrolment phase
S.Administrator	Authenticate as Administrator	ADMIN_RAD	Usage phase
S.Signatory	Compute SAD, IMPORT	DTBSR	Usage phase
S.Signatory	READ, Compute SAD, EXPORT	IDENTIFICATION_DATA_I	Usage phase
S.Signatory	Compute SAD, EXPORT	SIGNATORY_DATA	Usage phase
S.Signatory	Compute SAD	SAD_KEY	Usage phase
S.Signatory	GENERATE, DELETE	SAD	Usage phase
S.Signatory	COMPARE,	SIGNATORY_RAD	Usage phase

Subject	Operations	Objects	Comments / Phase
	CHANGE		
S.Signatory	Authenticate as Signatory, IMPORT	SIGNATORY_VAD_HOLDER-SIDE	Usage phase
S.Signatory	EXPORT, IMPORT	SIGNATORY_VAD_SERVER-SIDE	Usage phase
S.Signatory	EXECUTE	Commands performed after signatory authentication	Usage phase
S.User	EXECUTE	Commands performed prior signatory authentication	Usage phase

Table 12 - Subjects and Operations

Application note (*): Operations for Personalization phase are given here for information but not covered by SFR as this phase is prior TOE delivery.

List of TSP basic rules to be applied for each user are defined in the following table:

Subject	Rules
S.Signatory or S.Administrator	User is limited to restricted actions prior administrator or signatory authentication or if authentication fails. User is considered as S.Signatory as soon as signatory authentication succeeds. User is considered as S.Administrator as soon as Administration authentication succeeds. When authentication fails, number of authentication failure is incremented, and it must be done again [if still possible]. Number of authentication failure (retry counter) is limited. When maximum value of retry counter is reached, no more authentication can be done. Value of retry counter can be initialized only by change of RAD.
S.Signatory	Only S.Signatory can compute a SAD to be transmitted to SERVER. Only the Signatory can execute, import, export sign request Only the Signatory can compute, delete SAD Only the Signatory can import DTBSR Only the Signatory can export, read Identification Data Only the Signatory can export Signatory data Only the Signatory can change the signatory RAD
S.Communication_manager	SCC authentication can take place only when SERVER is authenticated. Data can be exchanged between SCC and SERVER only when secure channel is setup or to initiate the secure channel. Secure channel (data encryption and MAC calculation/verification) is setup only after SERVER and SCC are mutually authenticated.
S.Command_manager	Authorized commands depend on subject, secure state and current phase as defined in previous tables.
S.Administrator	Only S.Administrator can block SAD computation by deactivating RAD, or destroying SAD key. Only S.Administrator can perform operation restricted to administrator, as management of security attributes, key generation importation or destruction or RAD importation. Only the Administrator can import or generate SCC authentication Key Only the Administrator can import SERVER authentication Key(s) Only the Administrator can import or store SAD Key Only the Administrator can change phase from enrolment to usage

Subject	Rules
	Only S.Administrator can change or import ADMIN_RAD Only S.Administrator can store, import, activate and deactivate SIGNATORY_RAD Only S.Administrator can write, store, import identification data Only S.Administrator can import Signatory data

Table 13 - TSP Basic rules

7.1.2 Enrolment Phase

FDP_ACC.1/ENR Subset access control

FDP_ACC.1.1/ENR Subset access control The TSF shall enforce the ***[assignment: access control SFP]*** on ***[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]***.

The TSF shall enforce the **access control SFP during the Enrolment phase** on

- Subjects: **S.Command_Manager, S.Communication_Manager, Authorized S.Administrator**,
- Objects: **All objects defined in Table 12 during the Enrolment Phase, *[selection: none, [assignment: additional objects]]***
- Operations: **All operations defined in Table 12 during the Enrolment Phase, *[selection: none, [assignment: additional operations]]***

FDP_ACF.1/ENR Security attribute based access control

FDP_ACF.1.1/ENR Security attribute based access control The TSF shall enforce the **[access control SFP during the Enrolment phase]** to objects based on the following: **[all operations (during the Enrolment Phase) between subjects and objects defined in Table 12 based upon the attributes defined in Table 11, *[selection: none, [assignment: additional operations]]*]**.

FDP_ACF.1.2/ENR Security attribute based access control The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[all rules defined in Table 13 and received from an authorized S.Command_Manager, S.Communication_Manager, S.Administrator during the Enrolment Phase]**.

FDP_ACF.1.3/ENR Security attribute based access control The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/ENR Security attribute based access control The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[all rules defined in Table 13 and received from unauthorized S.Administrator during the Enrolment Phase, *[selection: none, [assignment: additional rules]]*].**

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

FDP_ITC.2.1/ENR_AUTH Import of user data with security attributes The TSF shall enforce the **[information flow control SFP during the Enrolment Phase]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/ENR_AUTH Import of user data with security attributes The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/ENR_AUTH Import of user data with security attributes 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/ENR_AUTH Import of user data with security attributes 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/ENR_AUTH Import of user data with security attributes The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[importation operations of Authentication user data (defined in Table 13, related to an Authorized S.Administrator during the Enrolment Phase) through a secure communication based upon the attribute AT.SecureChannel, *[selection: none, [assignment: additional rules]]*]**.

Application Note:

It includes: **SCC_AUTHENTICATION_SECRET_KEY, TSCM_AUTHENTICATION_PUB_KEY, SAP_HSM_AUTHENTICATION_PUB_KEY and SCC_AUTHENTICATION_PUB_KEY**.

FCS_CKM.1/AKey Cryptographic key generation

FCS_CKM.1.1/AKey Cryptographic key generation 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:
This component requires that the TOE be able to generate the Key(s) (Asymmetric or Symmetric) that are used for the SCC authentication according to OSP.CRYPTO. If the symmetric and the asymmetric cryptographic generation are supported, then the ST author should iterate this requirement to capture this capability.

FMT_MSA.1/ENR Management of security attributes

FMT_MSA.1.1/ENR Management of security attributes The TSF shall enforce the **[access control SFP during the Enrolment phase]** to restrict the ability to [**all operations defined in Table 12 during the Enrolment Phase, *[selection: none, [assignment: additional operations]]*]** the security attributes **[attributes defined in Table 11, *[selection: none, [assignment: additional security attributes]]*]** to **[S.Administrator, S.Command_manager, S.Communication_manager]**.

FMT_MSA.3/ENR Static attribute initialisation

FMT_MSA.3.1/ENR Static attribute initialisation The TSF shall enforce the **[access control SFP during the Enrolment phase]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ENR Static attribute initialisation The TSF shall allow the **[S.Administrator]** to specify alternative initial values to override the default values when an object or information is created.

Application Note:
Security Attributes are defined in Table 11.

FDP_ITC.2/ENR_SIGN Data Import of user data with security attributes

FDP_ITC.2.1/ENR_SIGN Data Import of user data with security attributes The TSF shall enforce the **[information flow control SFP during the Enrolment Phase]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/ENR_SIGN Data Import of user data with security attributes The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/ENR_SIGN Data Import of user data with security attributes 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/ENR_SIGN Data Import of user data with security attributes 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/ENR_SIGN Data Import of user data with security attributes The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[importation operations of signature user data (defined in Table 13, related to an Authorized S.Administrator during the Enrolment Phase) through a secure communication based upon the attribute AT.SecureChannel, *[selection: none, [assignment: additional rules]]*]**.

Application Note:

It includes **SIGNATORY_DATA**, **SAD_KEY** and **IDENTIFICATION_DATA_I**.

7.1.3 Usage Phase

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 User attribute definition The TSF shall maintain the following list of security attributes belonging to individual users: **[AT.SecureChannel, AT.Phase, AT.SecureState, AT.Authenticated_user*, [selection: none, [assignment: additional security attributes]]*]**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 Timing of authentication The TSF shall allow **[items provided in table 12 and 13, *[selection: none, [assignment: list of TSF mediated actions]]*]** on behalf of the user to be performed before the user is authenticated.

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

Application note: Table 12 provides list of operations and Table 13 provides list of rules.

FIA_UID.1 Timing of identification

FIA_UID.1.1 Timing of identification The TSF shall allow ***[assignment: list of TSF-mediated actions]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 Timing of identification 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 User-subject binding The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[AT.Authenticated_user*, [selection: Administrator, Signatory [assignment: additional user security attributes]]*]**.

Application note: See table 11 for attribute management.

FIA_USB.1.2 User-subject binding The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***[assignment: rules for the initial association of attributes]***.

FIA_USB.1.3 User-subject binding The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***[assignment: rules for the changing of attributes]***.

7.1.3.1 SCC authentication by the SERVER

FIA_API.1/SCC Authentication Proof of Identity

FIA_API.1.1/SCC The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [selection: TOE, [*assignment: object, authorized user or role*]] to an external entity.

7.1.3.2 SERVER Authentication by the TOE

FIA_AFL.1/SERVER Authentication failure handling Authentication failure handling

FIA_AFL.1.1/SERVER Authentication failure handling The TSF shall detect when **[selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]]** unsuccessful authentication attempts occur related to **[assignment: *list of authentication events*]**.

FIA_AFL.1.2/SERVER Authentication failure handling When the defined number of unsuccessful authentication attempts has been **[selection: *met, surpassed*]**, the TSF shall **[assignment: *list of actions*]**.

FIA_UID.1/SERVER Timing of identification

FIA_UID.1.1/SERVER Timing of identification The TSF shall allow ***[*to read AT.SecureChannel, AT.SecureState and AT.Authenticated_user, to verify the validity of the SERVER certificate (in case of Asymmetric key pair), to read the identification data of SERVER, *[selection: none, [assignment: list of TSF mediated actions]]*]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/SERVER Timing of identification The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/SERVER Timing of authentication

FIA_UAU.1.1/SERVER Timing of authentication The TSF shall allow **[to read AT.SecureChannel, AT.SecureState and AT.Authenticated_user, to verify the validity of the SERVER certificate (in case of Asymmetric key pair), to read the identification data of SERVER, *[selection: none, [assignment: list of TSF mediated actions]]*]** on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.4/SERVER Single-use authentication mechanisms

FIA_UAU.4.1/SERVER Single-use authentication mechanisms The TSF shall prevent reuse of authentication data related to **[SERVER authentication to SCC]**.

FIA_UAU.6/SERVER Re-authenticating

FIA_UAU.6.1/SERVER Re-authenticating The TSF shall re-authenticate the **SERVER** under the conditions **[terminated session due authentication failure, terminated session due to timeout, *[selection: none, [assignment: additional list of conditions under which re-authentication is required]]*]**.

7.1.3.3 Secure Channel between TOE and SERVER

FDP_ACC.1/SC Secure Channel Subset access control

FDP_ACC.1.1/SC Secure Channel Subset access control The TSF shall enforce the **[assignment: *access control SFP*]** on **[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]**.

The TSF shall enforce the **access control SFP during the Usage phase** on

- Subjects: **S.Communication_Manager**,
- Objects: **All objects defined in Table 12 and related to S.Communication_Manager, *[assignment: additional objects]***
- Operations: **All operations defined in Table 12 and related to S.Communication_Manager, *[assignment: additional operations]***

FDP_ACF.1/SC Secure Channel Security attribute based access control

FDP_ACF.1.1/SC Secure Channel Security attribute based access control The TSF shall enforce the **[access control SFP during the Usage phase]** to objects based on the following: **[all operations between subjects and objects defined in Table 12, related to S.Communication_Manager and based upon the attribute AT.SecureChannel, *[assignment: others]*]**.

FDP_ACF.1.2/SC Secure Channel Security attribute based access control The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[rules defined in Table 13 and related to S.Communication_Manager, *[assignment: additional rule]*]**.

FDP_ACF.1.3/SC Secure Channel Security attribute based access control The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1.4/SC Secure Channel Security attribute based access control The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

FDP_UCT.1/SC Basic data exchange confidentiality

FDP_UCT.1.1/SC Basic data exchange confidentiality The TSF shall enforce the **[information flow control SFP]** to **[*selection: transmit, receive*]** user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/SC Data exchange integrity

FDP_UIT.1.1/SC Data exchange integrity The TSF shall enforce the **[information flow control SFP]** to **[transmit, receive]** user data in a manner protected from **[modification, replay]** errors.

FDP_UIT.1.2/SC Data exchange integrity The TSF shall be able to determine on receipt of user data, whether **[modification, replay]** has occurred.

FTP_ITC.1/SC Inter-TSF trusted channel

FTP_ITC.1.1/SC Inter-TSF trusted channel The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SC Inter-TSF trusted channel The TSF shall permit **[the TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3/SC Inter-TSF trusted channel The TSF shall initiate communication via the trusted channel for **[sign request function, *[assignment: additional functions for which a trusted channel is required]*]**.

FDP_IFC.2/SC Complete information flow control

FDP_IFC.2.1/SC Complete information flow control The TSF shall enforce the **[information flow control SFP]** on **[Subject: Communication_Manager, Information: Signature request from TW4S, DTBSR, SCC identification data, *[assignment: additional subjects and information]*]** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/SC Complete information flow control The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1/SC Simple security attributes

FDP_IFF.1.1/SC Simple security attributes The TSF shall enforce the **[information flow control SFP]** based on the following types of subject and information security attributes: **[signature request from TW4S, DTBSR, SCC identification data managed by S.Communication_Manager during transfer between SCC and SERVER [*assignment:* *additional* ***subjects and information controlled under the indicated SFP, and for each, the security attributes***]**.

FDP_IFF.1.2/SC Simple security attributes The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[authorize exchange when secure channel is setup with SERVER by S.Communication_Manager]**.

FDP_IFF.1.3/SC Simple security attributes The TSF shall enforce the **[none]**.

FDP_IFF.1.4/SC Simple security attributes The TSF shall explicitly authorize an information flow based on the following rules: **[none]**.

FDP_IFF.1.5/SC Simple security attributes The TSF shall explicitly deny an information flow based on the following rules: **[none]**.

FMT_MSA.1/SC Management of security attributes

FMT_MSA.1.1/SC Management of security attributes The TSF shall enforce the **[access control SFP]** to restrict the ability to **[modify]** the security attributes **[AT.SecureChannel]** to **[S.Communication_Manager]**.

FMT_MSA.3/SC Static attribute initialization

FMT_MSA.3.1/SC Static attribute initialization The TSF shall enforce the **[access control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SC Static attribute initialization The TSF shall allow the **[S.Communication_Manager]** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

Security Attributes are defined in Table 11.

FPT_RPL.1/SC Replay detection

FPT_RPL.1.1/SC Replay detection The TSF shall detect replay for the following entities: **[messages exchanged between SERVER and SCC]**.

FPT_RPL.1.2/SC Replay detection The TSF shall perform **[denial of the request, close session and return an error to the user, *[assignment: other specific actions]*]** when replay is detected.

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

FPT_TDC.1.1/SC Inter-TSF basic TSF data consistency The TSF shall provide the capability to consistently interpret **[assignment: list of TSF data types]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SC Inter-TSF basic TSF data consistency The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

7.1.3.4 User authentication by the TOE

SFR for User authentication have been transferred in Appendix C for HOLDER-SIDE authentication and Appendix D for SERVER-SIDE authentication.

7.1.4 SAD Computation

FDP_ACC.1/SADComp SAD Computation Subset access control

FDP_ACC.1.1/SADComp SAD Computation Subset access control The TSF shall enforce the **[assignment: *access control SFP*]** on **[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]**.

The TSF shall enforce the **access control SFP during the Usage phase** on

- Subjects: **S.Command_Manager, Authorized S.Signatory**,
- Objects: **DTBSR, IDENTIFICATION_DATA_I, SIGNATORY_DATA, SAD_KEY, *[assignment: additional objects]***
- Operations: **Compute SAD**

FDP_ACF.1/SADComp Security attribute based access control

FDP_ACF.1.1/SADComp The TSF shall enforce the **[access control SFP during the Usage phase]** to objects based on the following: **[S.Signatory computes SAD by using DTBSR, IDENTIFICATION_DATA_I, SIGNATORY_DATA, SAD_KEY as input data for the computation, [*assignment: others]*]**.

FDP_ACF.1.2/SADComp The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[Only S.Signatory can compute a SAD to be transmitted to SERVER, *[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*]**.

FDP_ACF.1.3/SADComp The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[The Signatory shall be successfully authenticated before allowing the computation of SAD]**.

FDP_ACF.1.4/SAD Comp the TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

FCS_COP.1/SAD Cryptographic operation

FCS_COP.1.1/SAD 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:

This component requires that the TOE be able to compute SAD. The ST author should iterate this requirement to capture this capability.

A recommended implementation for FCS_COP.1.1/SAD is standard OCRA: OATH Challenge-Response Algorithm described in [RFC6287].

In such case, for a secure SAP, SAD is computed as a HMAC based on SHA256 with an AES key on at least 128bits. Input for computation shall include at least DTBSR, a link with SCD identifier and a link with Signatory identifier.

7.1.5 Protection of the TSF

FCS_CKM.4/Akey Authentication key Cryptographic key destruction

FCS_CKM.4.1/Aky Authentication key Cryptographic key destruction 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: Relevant assets are **SCC_AUTHENTICATION_SecretKey, SCC_AUTHENTICATION_PubKey, SAP_HSM_AUTHENTICATION_PubKey.**

FCS_CKM.4/SAD_Key Cryptographic key destruction

FCS_CKM.4.1/SAD_key Cryptographic key destruction 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: Relevant assets are **SAD_KEY.**

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1Subset residual information protection The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***[selection: allocation of the resource to, deallocation of the resource from, both]*** the following objects: **[D.SIGNATORY_DATA, D.SAD, D.ADMIN_RAD *[selection: none, [assignment: additional objects]]*]**.

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1Stored data integrity monitoring and action The TSF shall monitor user data stored in containers controlled by the TSF for ***[assignment: integrity errors]*** on all objects, based on the

following attributes: **[user data objects defined in Table 11, *[selection: none, [assignment: additional user data objects]]*]**.

FDP_SDI.2.2Stored data integrity monitoring and action upon detection of a data integrity error, the TSF shall **[prohibit the use of the altered data, send back an error message, *[selection: none, [assignment: additional actions to be taken]]*]**.

FDP_SDC.2 Stored data confidentiality by type

FDP_SDI.2.1Stored data confidentiality by type The TSF shall ensure the confidentiality of the information of the user data according to [***assignment: data type***] while it is stored in the TOE.

Application note: ST writer will refine such requirements according to supported data type.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[*assignment: access control SFP(s), information flow control SFP(s)*]** to restrict the ability to **[*selection: change_default, query, modify, delete, [assignment: other operations]*]** the security attributes **[*assignment: list of security attributes*]** to **[S.Command_Manager, S.Communication_Manager and S.Signatory]**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 Secure security attributes The TSF shall ensure that only secure values are accepted for **[security attributes defined in Table 11, *[assignment: other security attributes]*]**.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 Static attribute initialization The TSF shall enforce the **[*assignment: access control SFP, information flow control SFP*]** to provide **[restrictive,]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 Static attribute initialization The TSF shall allow the **[S.Administrator]** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

Refer to Table 11 for the list of security attributes.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 Management of TSF data The TSF shall restrict the ability to **[*selection: change_default, query, modify, delete, clear, [assignment: other operations*]]** the **[*assignment: list of TSF data*]** to **[*assignment: the authorized identified roles*]**.

Application Note:

Refer to Table 13 for the list of rules.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 Specification of management functions The TSF shall be capable of performing the following management functions: **[assignment: *list of management functions to be provided by the TSF*]**.

Refer to Table 12 for the list of management functions.

FMT_SMR.1 Security roles

FMT_SMR.1.1Security roles The TSF shall maintain the roles **[S.Administrator, S.Command_Manager, S.Communication_Manager, and S.Signatory]**.

FMT_SMR.1.2Security roles The TSF shall be able to associate users with roles.

FPT_FLS.1Failure with preservation of secure state

FPT_FLS.1.1Failure with preservation of secure state The TSF shall preserve a secure state when the following types of failures occur: **[failure during key generation operation, failure during the SAD computation, failure during SCC authentication, failure during SERVER authentication, *[assignment: additional types of failures in the TSF]*]**.

7.2 Security Assurance Requirements

The selected package of security assurance requiments is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5. List of comments is listed in table below and details are in [CC3].

Assurance Class	Requirements
Development ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance Documents AGD	AGD_OPE.1
	AGD_PRE.1
Life cycle support ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
Security Target evaluation ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment AVA	AVA_VAN.5

Table 14 - List of Security Assurance Requirements

7.3 Security Requirements Rationale

7.3.1 Security Objectives for the TOE

OT.AUTHENTICATION_KEY_IMPORT

This security objective is satisfied by the following SFRs which guarantee that the import of the SCC and SERVER Authentication Key(s) are secure and protected against disclosure and modification:

- FDP_ACC.1/ENR, FDP_ACF.1/ENR define the access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE during the enrolment phase.
- FDP_ITC.2/ENR_AUTH requires the TSF to import Authentication user data and keys unambiguously associated with their security attributes by an authorized Administrator during the Enrolment Phase through a secure communication.
- FMT_MSA.1/ENR ensures that the authorized subject manages security attributes applied to access control and information flow control policies during the enrolment phase.
- FMT_MSA.3/ENR provides default values of security attributes applied to access control and information flow control policies.
- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data
- FIA_ATD.1 defines the security attribute list for administrator that are used for key importation.
- FIA_UAU.1 ensures the ability to define the list of administrator operations (as key importation) allowed prior and after administrator authentication is performed.
- FIA_UID.1 states that the Administrator has to be successfully identified before performing any action.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role. The administrator role is associated to enrolment operations.
- FMT_SMF.1 requires to specify management functions as key importation such as security attributes, TSF data and security functions, etc., to be executed by TSF.

OT.AUTHENTICATION_KEY_GENERATE

This security objective is satisfied by the following SFRs which provide the generation of SCC authentication key, the export of public key in the case of use of Asymmetric key generation in order to request the generation of SCC Authentication certificate:

- FCS_CKM.1/AKey requires the TOE to generate cryptographic strong keys needed for the SCC Authentication using Endorsed cryptographic key generation algorithms.
- FMT_MSA.1/ENR ensures that the authorized subject manages security attributes applied to access control and information flow control policies during the enrolment phase.
- FMT_MSA.3/ENR provides default values of security attributes applied to access control and information flow control policies.

- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role. The administrator role is associated to enrolment operations.

OT.SIGNATORY_IDDATA_ENR

This security objective is satisfied by the following SFRs which provide the importation of Signatory Identification data:

- FMT_MSA.3/ENR provides default values of security attributes applied to access control and information flow control policies.
- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role. The administrator role is associated to enrolment operations.

OT.SCD_ID_IMPORT

This security objective is satisfied by the following SFRs which guarantee that the import of the SCD Identification Data is secure:

- FDP_ITC.2/ENR_SIGN requires the TSF to import signature user data and keys unambiguously associated with their security attributes by an authorized Administrator during the Enrolment Phase through a secure communication.
- FDP_ACC.1/ENR, FDP_ACF.1/ENR define the access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE during the enrolment phase.
- FMT_MSA.1/ENR ensures that the authorized subject manages security attributes applied to access control and information flow control policies during the enrolment phase.
- FMT_MSA.3/ENR provides default values of security attributes applied to access control and information flow control policies.
- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data.
- FIA_ATD.1 defines the security attribute list for administrator that are used for sensitive data importation.
- FIA_UAU.1 ensures the ability to define the list of administrator operations (as for sensitive data importation) allowed prior and after administrator authentication is performed.
- FIA_UID.1 states that the Administrator has to be successfully identified before performing any action.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role. The administrator role is associated to enrolment operations.
- FMT_SMF.1 requires to specify management functions as key importation such as security attributes, TSF data and security functions, etc., to be executed by TSF.

OT.SAD_KEY_IMPORT This security objective is satisfied by the following SFRs which guarantee that the import of the SAD KEY is secure:

- FDP_ACC.1/ENR, FDP_ACF.1/ENR define the access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE during the enrolment phase.
- FDP_ITC.2/ENR_SIGN requires the TSF to import signature user data and keys unambiguously associated with their security attributes by an authorized Administrator during the Enrolment Phase through a secure communication.
- FMT_MSA.1/ENR ensures that the authorized subject manages security attributes applied to access control and information flow control policies during the enrolment phase.
- FMT_MSA.3/ENR provides default values of security attributes applied to access control and information flow control policies.
- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data
- FIA_ATD.1 defines the security attribute list for administrator that are used for key importation.
- FIA_UAU.1 ensures the ability to define the list of administrator operations (as for key importation) allowed prior and after administrator authentication is performed.
- FIA_UID.1 states that the Administrator has to be successfully identified before performing any action.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role. The administrator role is associated to enrolment operations.
- FMT_SMF.1 requires to specify management functions as key importation such as security attributes, TSF data and security functions, etc., to be executed by TSF.

OT.SCC_AUTHENTICATION

This security objective is satisfied by the following SFRs which impose that the TOE shall provide information to SERVER to be authenticated and shall implement cryptographic protocol for the SCC authentication:

- FIA_ATD.1 defines the security attribute list for each authorized subject that are also used for authentication and signature mechanisms.
- FIA_API.1/SCC ensures that computation of data is performed for a successful SCC authentication by SERVER
- FDP_ACC.1/SC, FDP_ACF.1/SC defines the secure channel access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE.
- FMT_MSA.1/SCC ensures that the authorized subject manages security attributes applied to access control for secure channel management.
- FMT_MSA.3/SCC provides default values of security attributes applied to access control and information flow control policies for secure channel management.

OT.SERVER_AUTHENTICATION

This security objective is satisfied by the following SFRs which impose that the TOE shall provide mechanism(s) to authenticate SERVER and shall not deliver data to SERVER before SERVER authentication by the TOE:

- FIA_ATD.1 defines the security attribute list for each authorized subject that are also used for authentication and signature mechanisms.
- FIA_AFL.1/SERVER ensures the ability to define the behavior in case of authentication failure.
- FIA_UID.1/SERVER ensures that a successful SCC identification to SERVER is performed before any other TSF mediated actions may take place.
- FIA_UAU.1/SERVER ensures that a successful SCC authentication to SERVER is performed before any other TSF mediated actions may take place.
- FIA_UAU.4/SERVER ensures the ability to prevent reusing of SCC authentication data**,**
- FIA_UAU.6/SERVER requires re-authentication after terminated session of the TOE due to authentication failure or session timeout.

OT.SECURE_CHANNEL

This security objective is satisfied by the following SFRs which impose that the TOE shall be able to create a secure channel with SERVER and to manage it to assure integrity and optionally confidentiality of data exchange:

- FDP_ACC.1/SC, FDP_ACF.1/SC defines the secure channel access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE.FDP_UCT.1/SC addresses the protection of the data containing confidential information during data exchange.
- FDP_UIT.1/SC addresses the protection of the data containing integrity sensitive information during data exchange.
- FIA_ATD.1 defines the security attribute list including [AT.SecureChannel] used for secure channel management.
- FTP_ITC.1/SC requires that the TSF provides a communication channel between itself and SERVER. The channel provides assured identification of its end points and protection of the channel data against modification and disclosure.
- FDP_IFC.2/SC ensures that security policy for the TOE information flow control when secure channel is setup with SERVER is defined.
- FDP_IFF.1/SC provides the rules to control information flow when secure channel is setup with SERVER on the basis of security attributes.
- FMT_MSA.1/SC ensures that the authorized subject manages security attributes applied to access control and information flow control policies when secure channel is setup with SERVER.
- FMT_MSA.3/SC provides default values of security attributes applied to access control and information flow control policies when secure channel is setup with SERVER. Alternative default values for these security attributes shall only be allowed for dedicated authorized roles.
- FPT_RPL.1/SC ensures that replaying will be detected for the signature request received from SCA and transmitted to SERVER. When replay is detected, the TSF will perform a denial of the request and return an error to the user.

- FPT_TDC.1/SC the TOE provides an authentication functionality to consistently interpret data when shared between the TSF and SERVER and uses roles when interpreting this data.
- FDP_RIP.1 TOE performs residual information protection for data exchange in the secure channel

  FDP_SDI.2 TOE performs monitoring of integrity of stored Keys used in secure channel

OT.SIGN_ACTIVATION_PROTECTION

This security objective is satisfied by the following SFRs which impose that the TOE shall avoid any bypass of security operations (SCC authentication and SAD computation, Signature request transfer etc.):

- FDP_ACC.1/SADComp, FDP_ACF.1/SADComp defines the SAD computation access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE,
- FMT_MSA.1 restricts the ability to manage the security attributes to authorized roles,
- FMT_MSA.2 ensures that only authorized value inside limits of TSF data and takes handling actions when the indicated limits are reached or exceeded,
- FMT_MSA.3 provides default values of security attributes applied to access control and information flow control policies.

OT.DTBSR_SAD_INTEGRITY

This security objective is satisfied by the following SFR which imposes that the TOE shall assure integrity of SAD during SAD computation and transmission to SERVER:

- FCS_COP.1/SAD requires the necessary cryptographic operations needed for SAD computation.

OT.SAD_COMPUTATION

This security objective is satisfied by the following SFR which imposes that the TOE shall compute unique SAD for each signature request to protect against replay:

- FCS_COP.1/SAD requires the necessary cryptographic operations needed for SAD computation.

OT.PROTECTION

This security objective is satisfied by the following SFRs which impose that the TOE shall protect any sensitive data stored in SCC against unauthorized disclosure and /or modification:

- FCS_CKM.4/AKey ensures that authentication key(s) are securely destroyed in accordance with a given specific key destruction method when they are no longer needed for correct operation of the TOE.
- FCS_CKM.4/SAD_key ensures that SAD key is securely destroyed in accordance with a given specific key destruction method when they are no longer needed for correct operation of the TOE.
- FDP_RIP.1 requires that residual information regarding sensitive data in previously used resources will not be available after its usage.

- FDP_SDI.2 requires the TSF to monitor user data stored in containers and to take assigned action when data integrity error is detected.
- FDP_SDC.2 requires the TSF to monitor user data stored in containers and to take assigned action when data confidentiality is required.
- FPT_FLS.1 requires the preservation of a secure state at failure situations in order to protect the user data, TSF data and security services.

OT.CRYPTO

This security objective is satisfied by the following SFRs which impose that the TOE shall implement cryptographic functions that are recommended by the Certification Body:

- FCS_COP.1/SAD requires the necessary cryptographic operations needed for SAD computation.
- FIA_API.1/SCC requires the necessary cryptographic operations needed for computation of data for a successful SCC authentication by SERVER
- FDP_UCT.1/SC addresses the protection of the data containing confidential information during data exchange.
- FDP_UIT.1/SC addresses the protection of the data containing integrity sensitive information during data exchange.
- FTP_ITC.1/SC requires that the TSF provides a communication channel between itself and SERVER. The channel provides assured identification of its end points and protection of the channel data against modification and disclosure.
- FIA_UAU.1/SERVER requires the necessary cryptographic operations for SERVER authentication
- FIA_UAU.4/SERVER requires the necessary cryptographic operations for SERVER authentication
- FIA_UAU.6/SERVER requires the necessary cryptographic operations for SERVER re-authentication.

7.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.AUTHENTICATION_KEY_IMPORT	FDP_ACC.1/ENR Subset access control, FDP_ACF.1/ENR Security attribute based access control, FDP_ITC.2/ENR_AUTH Import of user data with security attributes, FMT_MSA.1/ENR Management of security attributes, FMT_MSA.3/ENR, FMT_MTD.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1	

OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation	FCS_CKM.1/AKP Cryptographic key generation, FMT_MSA.1/ENR Management of security attributes, FMT_MSA.3/ENR Static Initialization of security attributes, FMT_MTD.1, FMT_SMR.1, FIA_ATD.1	
OT.SIGNATORY_IDDATA_ENR	FMT_MSA.3/ENR Static Initialization of security attributes, FMT_MTD.1, FMT_SMR.1	
OT.SCD_ID_IMPORT SCD Identification Data Import	FDP_ITC.2/ENR_SIGN Import of user data with security attributes, FDP_ACC.1/ENR, FDP_ACF.1/ENR, FMT_MSA.1/ENR, FMT_MSA.3/ENR FMT_MTD.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1	
OT.SADKEY_IMPORT SAD Key Import	FDP_ITC.2/ENR_SIGN Data Import of user data with security attributes, FDP_ACC.1/ENR Subset access control, FDP_ACF.1/ENR Security attribute based access control, FMT_MSA.1/ENR Management of security attributes, FMT_MSA.3/ENR Static Initialization of security attributes, FMT_MTD.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1	
OT.SCC_AUTHENTICATION SCC Authentication data for SERVER	FDP_ACC.1/SC Subset access control, FDP_ACF.1/SC Security attribute based access control, FMT_MSA.1/SC Management of security attributes, FMT_MSA.3/SC Static Initialization of security attributes, FIA_ATD.1, FIA_API.1/SCC	
OT.SERVER_AUTHENTICATION SERVER Authentication by TOE	FIA_ATD.1, FIA_AFL.1/SERVER, FIA_UID.1/SERVER, FIA_UAU.1/SERVER, FIA_UAU.4/SERVER, FIA_UAU.6/SERVER	

OT.SECURE_CHANNEL Secure channel between SERVER and TOE	FIA_ATD.1 User attribute definition, FDP_ACC.1/SC, FDP_ACF.1/SC, FDP_UCT.1/SC, FDP_UIT.1/SC, FTP_ITC.1/SC, FDP_IFC.2/SC FDP_IFF.1/SC, FMT_MSA.1/SC, FMT_MSA.3/SC, FPT_RPL.1/SC, FPT_TDC.1/SC	
OT.SIGN_ACTIVATION_PROTECTION Access Control to SAD Computation	FDP_ACC.1/SADComp, FDP_ACF.1/SADComp, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3	
OT.DTBSR_SAD_INTEGRITY DTBSR and SAD Integrity	FCS_COP.1/SAD	
OT.SAD_COMPUTATION SAD Computation For Signature Operation Anti Replay	FCS_COP.1/SAD	
OT.PROTECTION Sensitive Data Protection	FCS_CKM.4/AKey, FCS_CKM.4/SAD_key, FDP_RIP.1, FDP_SDI.2, FDP_SDC.2, FPT_FLS.1	
OT.CRYPTO	FCS_COP.1/SAD, FIA_API.1/SCC, FDP_UCT.1/SC, FDP_UIT.1/SC, FTP_ITC.1/SC, FIA_UAU.1/SERVER, FIA_UAU.4/SERVER, FIA_UAU.6/SERVER	

Table 15 - Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	Rationale
FDP_ACC.1/ENR	OT.AUTHENTICATION_KEY_IMPORT SCC AUTH Key Import, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT	
FDP_ACF.1/ENR Security attribute based access control	OT.AUTHENTICATION_KEY_IMPORT SCC AUTH Key Import, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT	
FCS_CKM.1/AKey Cryptographic key generation	OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation	
FDP_ITC.2/ENR_AUTH	OT.AUTHENTICATION_KEY_IMPORT SCC AUTH Key Import	

FMT_MSA.1/ENR Management of security attributes	OT.AUTHENTICATION_KEY_IMPORT SCC AUTH Key Import, OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation, OT.SCD_ID_IMPORT SCD Identification Data Import, OT.SAD_KEY_IMPORT	
FMT_MSA.3/ENR Static initialization of security attributes	OT.AUTHENTICATION_KEY_IMPORT SCC AUTH Key Import, OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation, OT.SIGNATORY_IDDATA_ENR, OT.SCD_ID_IMPORT SCD Identification Data Import, OT.SAD_KEY_IMPORT	
FDP_ITC.2/ENR_SIGN Data Import of user data with security attributes	OT.SCD_ID_IMPORT SCD Identification Data Import, OT.SAD_KEY_IMPORT	
FIA_ATD.1User attribute definition	OT.AUTHENTICATION_KEY_IMPORT, OT.SERVER_AUTHENTICATION, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT, OT.SCC_AUTHENTICATION, OT.SECURE_CHANNEL	
FIA_UID.1 Timing of Identification	OT.AUTHENTICATION_KEY_IMPORT, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT, OT.USER_AUTHENTICATION_HOLDER-SIDE User Authentication by TOE, OT.USER_AUTHENTICATION_SERVER-SIDE SERVER-SIDE User Authentication by TOE	
FIA_USB.1 User-subject binding	OT.AUTHENTICATION_KEY_IMPORT, OT.SIGNATORY_IDDATA_ENR,	
FIA_UAU.1 Timing of authentication	OT.AUTHENTICATION_KEY_IMPORT, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT,	
FIA_API.1/SCC Authentication Proof of Identity	OT.SCC_AUTHENTICATION, OT.USER_AUTHENTICATION_HOLDER-SIDE, OT.USER_AUTHENTICATION_SERVER-SIDE SERVER-SIDE, OT.CRYPTO	
FIA_AFL.1/SERVER Authentication failure handling	OT.SERVER_AUTHENTICATION, OT.AUTHENTICATION_KEY_IMPORT, OT.SIGNATORY_IDDATA_ENR,	
FIA_UID.1/SERVER Timing of Identification	OT.SERVER_AUTHENTICATION, OT.USER_AUTHENTICATION_HOLDER-SIDE User Authentication by TOE, OT.USER_AUTHENTICATION_SERVER-SIDE SERVER-SIDE User Authentication by TOE	
FIA_UAU.1/SERVER Timing of authentication	OT.AUTHENTICATION_KEY_IMPORT, OT.SIGNATORY_IDDATA_ENR, OT.SERVER_AUTHENTICATION, OT.CRYPTO	
FIA_UAU.4/SERVER Single-use authentication mechanisms	OT.CRYPTO OT.SERVER_AUTHENTICATION,	

FIA_UAU.6/SERVER Re-authenticating	OT.USER_AUTHENTICATION_HOLDER-SIDE, OT.USER_AUTHENTICATION_SERVER-SIDE SERVER-SIDE, OT.SERVER_AUTHENTICATION, OT.CRYPTO	
FDP_ACC.1/SC Secure Channel Subset access control	OT.SCC_AUTHENTICATION, OT.SERVER_AUTHENTICATION, OT.SECURE_CHANNEL	
FDP_ACF.1/SC Secure Channel Security attribute based access control	OT.SCC_AUTHENTICATION, OT.SERVER_AUTHENTICATION, OT.SECURE_CHANNEL	
FDP_UCT.1/SC Basic data exchange confidentiality	OT.SERVER_AUTHENTICATION, OT.CRYPTO, OT.SECURE_CHANNEL	
FDP_UIT.1/SC Data exchange integrity	OT.SERVER_AUTHENTICATION, OT.CRYPTO, OT.SECURE_CHANNEL	
FTP_ITC.1/SC Inter-TSF trusted channel	OT.SERVER_AUTHENTICATION, OT.CRYPTO, OT.SECURE_CHANNEL	
FDP_IFC.2/SC Complete information flow control	OT.SERVER_AUTHENTICATION, OT.SECURE_CHANNEL	
FDP_IFF.1/SC Simple security attributes	OT.SERVER_AUTHENTICATION, OT.SECURE_CHANNEL	
FMT_MSA.1/SC Management of security attributes	OT.SCC_AUTHENTICATION SCC Authentication data for SERVER, OT.USER_AUTHENTICATION User Authentication by TOE, OT.SECURE_CHANNEL	
FMT_MSA.3/SC Static attribute initialisation	OT.SCC_AUTHENTICATION SCC Authentication data for SERVER, OT.USER_AUTHENTICATION User Authentication by TOE, OT.SECURE_CHANNEL	
FPT_RPL.1/SC Replay detection	OT.SECURE_CHANNEL	
FPT_TDC.1/SC Inter-TSF basic TSF data consistency	OT.SECURE_CHANNEL	
FDP_ACC.1/SADComp SAD Computation Subset access control	OT.SIGN_ACTIVATION_PROTECTION	
FDP_ACF.1/SADComp	OT.SIGN_ACTIVATION_PROTECTION	
FCS_COP.1/SAD	OT.CRYPTO, OT.DTBSR_SAD_INTEGRITY, OT.SAD_COMPUTATION	
FCS_CKM.4/AKey Authentication key Cryptographic key destruction	OT.PROTECTION	
FCS_CKM.4/SAD_key Cryptographic key destruction	OT.PROTECTION	
FDP_RIP.1Subset residual information protection	OT.PROTECTION	

FDP_SDI.2 Stored data integrity monitoring and action	OT.PROTECTION	
FDP_SDC.2Stored data confidentiality	OT.PROTECTION	
FMT_MSA.1 Management of security attributes	OT.SIGN_ACTIVATION_PROTECTION Access Control to SAD Computation	
FMT_MSA.2 Secure security attributes	OT.SIGN_ACTIVATION_PROTECTION, , OT.CRYPTO Cryptographic Operations	
FMT_MSA.3 Static attribute initialization	OT.SIGN_ACTIVATION_PROTECTION, OT.PROTECTION Sensitive Data Protection	
FMT_MTD.1	OT.AUTHENTICATION_KEY_IMPORT, OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation, OT.SIGNATORY_IDDATA_ENR, OT.SCD_ID_IMPORT, OT.PROTECTION Sensitive Data Protection	
FMT_SMF.1	OT.AUTHENTICATION_KEY_IMPORT, OT.SCD_ID_IMPORT, OT.SAD_KEY_IMPORT, OT.PROTECTION Sensitive Data Protection	
FMT_SMR.1	OT.AUTHENTICATION_KEY_IMPORT, OT.AUTHENTICATION_KEY_GENERATE SCC AUTH Key Generation, OT.SAD_KEY_IMPORT, OT.SIGNATORY_IDDATA_ENR, OT.SCD_ID_IMPORT, OT.PROTECTION Sensitive Data Protection	
FPT_FLS.1Failure with preservation of secure state	OT.PROTECTION Sensitive Data Protection	

Table 16 - SFRs and Security Objectives

7.3.3 Dependencies

7.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/ENR	(FDP_ACF.1)	FDP_ACF.1/ENR
FDP_ACF.1/ENR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ENR, FMT_MSA.3/ENR
FDP_ITC.2/ENR_AUTH	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/ENR, see rationale next §
FCS_CKM.1/AKey	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	see rationale next §
FMT_MSA.1/ENR	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ENR, FMT_SMF.1, FMT_SMR.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.3/ENR	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ENR, FMT_SMR.1
FDP_ITC.2/ENR_SIGN	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/ENR, FPT_TDC.1/SC, FTP_ITC.1/SC
FIA_ATD.1	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_USB.1	(FIA_ATD.1)	FIA_ATD.1
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_API.1/SCC	No Dependencies	
FIA_AFL.1/ SERVER	(FIA_UAU.1)	FIA_UAU.1/SERVER
FIA_UID.1/SERVER	No Dependencies	
FIA_UAU.1/SERVER	(FIA_UID.1)	FIA_UID.1/SERVER
FIA_UAU.4/SERVER	No Dependencies	
FIA_UAU.6/SERVER	No Dependencies	
FDP_ACC.1/SADComp	(FDP_ACF.1)	FDP_ACF.1/SADComp
FDP_ACF.1/SADComp	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SADComp, FMT_MSA.3
FCS_COP.1/SAD	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/ENR_SIGN, FCS_CKM.4/SAD_key
FDP_ACC.1/SC	(FDP_ACF.1)	FMT_MSA.3/ENR, FDP_ACF.1/SC
FDP_ACF.1/SC	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SC, FMT_MSA.3/SC
FDP_UCT.1/SC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SC, FTP_ITC.1/SC
FDP_UIT.1/SC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SC, FTP_ITC.1/SC
FTP_ITC.1/SC	No Dependencies	
FDP_IFC.2/SC	(FDP_IFF.1)	FDP_IFF.1/SC
FDP_IFF.1/SC	(FDP_IFC.2) and (FMT_MSA.3)	FDP_IFC.2/SC, FMT_MSA.3/SC
FMT_MSA.1/SC	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SC, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3/SC	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/SC , FMT_SMR.1
FPT_RPL.1/SC	No Dependencies	
FPT_TDC.1/SC	No Dependencies	

FCS_CKM.4/AKey	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/Akey
FCS_CKM.4/SAD_key	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/ENR_SIGN
FDP_RIP.1	No Dependencies	
FDP_SDI.2	No Dependencies	
FDP_SDC.2	No Dependencies	
FMT_MSA.1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ENR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/ENR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No Dependencies	

Table 17 - SFRs Dependencies

7.3.3.1.1 Rationale for the exclusion of dependencies Requirements

The dependency FCS_CKM.2 or FCS_COP.1 introduced by the component FCS_CKM.1/AKey is considered to be satisfied because it is covered from the environment (Platform: OE.CRYPTO).

The dependency FPT_TDC.1 introduced by the component FDP_ITC.2/ENR_AUTH is considered to be satisfied because it is covered from the environment (OE.TRUSTED_TW4S TW4S, OE.TRUSTED_PERSO_ENROLMENT).

The dependency FTP_ITC.1 or FTP_TRP.1 introduced by the component FDP_ITC.2/ENR_AUTH is considered to be satisfied because it is covered from the environment (OE.TRUSTED_TW4S TW4S, OE.TRUSTED_PERSO_ENROLMENT).

7.3.3.2 SARs Dependencies

The following table lists SAR dependencies and the satisfied ones.

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4

AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.1, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 18 - SARs Dependencies

7.3.4 Rationale for the Security Assurance Requirements

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

7.3.5 ALC_DVS.2 Sufficiency of Security Measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the nature of the TOE, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

7.3.6 AVA_VAN.5 Advanced Methodical Vulnerability Analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for sensitive applications, in particular in payment and identity areas. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL4.

8 Glossary and Acronyms

Term	Definition
Authentication	Provision of assurance in the identity of an entity.
Authentication Factor	Piece of information and/or process used to authenticate or verify the identity of an entity
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Record by the operator of activities of the platform allowing a complete audit of the solution.
Authenticity	Ability to confirm the local part of the solution, comprising the SCC is authentic and can therefore be safely used by the user to authorize the use of his centrally stored key.
Data To Be Signed (DTBS)	data (e.g. a document or parts of a document) to be signed as well as any signature attributes that are bound together with the data by the signature NOTE Data To Be Signed is the input to the cryptographic signing algorithm. The specific way that Data To Be Signed and any signature attributes are fed as input is defined in the specifications of the signature type in use
Data To Be Signed Representation (DTBS/R)	data (e.g. a document or parts of a document) to be signed as well as any signature attributes that are bound together with the data by the signature NOTE Data To Be Signed is the input to the cryptographic signing algorithm. The specific way that Data To Be Signed and any signature attributes are fed as input is defined in the specifications of the signature type in use
Enrolment	The process of collecting user data (as biometric samples, if any) from a person and the subsequent preparation and storage of such data (as biometric reference templates) representing that person's identity. See [ISO-24760]
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. See [ISO-24760]
Integrity	Ability to confirm the TOE and its data elements on the chip have not been altered from that created by the issuing entity
Reference authentication data (RAD)	means data (PIN code or biometrics authentication reference) persistently stored by the TOE and used to identify authenticate a user as its signatory (integrity and confidentiality of RAD must be maintained)
Remote Signature Creation Device	Signature creation device using secure electronic communication channels, in order to guarantee that the signature creation environment is reliable and is used under the sole control of the signatory
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4. See [ISO-7816-4]
Signatory	Natural person or a legal person who creates a digital signature
Signature Activation Protocol (SAP)	Protocol designed to authorize signature operation on a given DTBS or DTBS/R using a signature creation data associated to a signatory. This process is defined in order to keep the DTBS or DTBS/R signature operation under sole control of the signatory even if it is done remotely on a server out of his control
Signature Activation Data (SAD)	Set of data (or derivate thereof), linked with a high level of confidence to the signature creation data, a DTBS or DTBSR and the signatory, which is used in a signature activation protocol
Signature Creation Application	Application that creates a signed document, using the digital signature produced by an SCDev connected to the SCA
Signature Generation Service	Trust Service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of digital

Term	Definition
Provider	signatures by means of such a remotely managed device
Trust Service Provider	A natural or a legal person who provides one or more trust services. There are qualified and non-qualified trust service providers
Trustworthy System Supporting Server Signing	Client-server system using SCD under sole control of the signatory, in order to create digital signatures
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC1]).
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [CC1]).
Verification	The process of comparing a submitted data (as biometric sample) against the reference (as biometric template) of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. See [ISO-24760]
Verification authentication data (VAD)	means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity. See [ISO-24760]

Acronym	Term
AKey	Authentication Key
APSD	Authentication Protocol Sensitive Data
CA	Certificate Authority
CC	Common Criteria
CM	Cryptographic Module
CGA	Certificate Generation Application
CSP	Credential Service Provider
CSP Credential	Credential Service Provider, issuing and managing the hardware, software, and associated data that can be used to produce credentials as Pin, Passwords and biometric or private keys stored in smart cards used for authentication purpose.
DTBS	Data To Be Signed
DTBSR	Data To Be Signed Representation
EAL	evaluation assurance level
EC	European Commission
LoA	Level of Assurance
n.a.	Not applicable
OBKG	On-Board Key Generation
OSP	Organizational security policy
PC	Personal Computer
PIN	Personal Identification Number
PP	Protection Profile
PT	Personalization Terminal
RAD	Reference Authentication Data
SAD	Signature Activation Data
SAD_Key	Key used for generation of SAD
SAP	Signature Activation Protocol

Acronym	Term
SAP HSM	SAP HSM module to perform access control to signature operation performed by cryptographic module (HSM)
SAR	Security Assurance Requirements
SCA	Signature Creation Application
SCC	Single Control Component part of T4WS
SCD	Signature Creation Data
SCD ID	SCD identifier
SD	Signers' Document
SDO	Signed data object
SFR	Security functional requirement
SSCD	Secure Signature Creation Device
ST	Security Target
TOE	Target of Evaluation
TSCM	A Trustworthy Signature Creation Module, distant IT system performing signature operation request only after control that SAP conditions are achieved.
TSF	TOE security functions
TW4S	Trustworthy System Supporting Server Signing
VAD	Verification Authentication Data

9 Literature

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Common Criteria [CC]

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[CCM] CC and CEM addenda, modular PP; CCMB-2014-03-001, Version 1.0, March 2014

ISO / CEN

[EN-419241] Security Requirements for Trustworthy Systems Supporting Server Signing - Part 1

[ISO-27115] ISO/IEC JTC 1/SC 27 Information technology — Security techniques — Entity authentication assurance framework – December 2012 - ISO/IEC FDIS 29115: 2012
[ISO-24760] ISO/IEC 24760-1:2011, Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.
[ISO-7816-4] ISO/IEC 7816-4:2013, Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange.
[ISO-29115] ISO/IEC 29115:2013, Information Technology – Security Techniques – Entity Authentication Assurance Framework.

Cryptography

[RFC6287] OCRA: OATH Challenge-Response Algorithm

Protection Profiles

[PP BSI-0084] Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, January 2014, BSI-PP-0084-2014
[PP SAP HSM] Protection profile for SAP HSM module in TW4S
[PP JCS Closed] Java Card Protection Profile – Closed Configuration, ANSSI-PP-2010-07
[PP JCS Open] Java Card Protection Profile – Open Configuration, ANSSI-PP-2010-03
[PP TEE] GlobalPlatform Device Committee TEE Protection Profile V1.0

[PP SAP] Protection profile on Signature Activation Protocol (SAP) management
[PP TSCM] Protection profile for Trustworthy Signature Creation Module in TW4S
[CEN 419221-5] Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services
[EAC2-PP] Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, BSI-CC-PP-0086
[MR.ED-PP] Machine-Readable Electronic Documents based on BSI TR-03110 for Official use,

BSI-CC-PP-0087

Others

[REGULATION] 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

[TR-03110] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents

Appendix A: ADMINISTRATION Group module PP

This Appendix introduces the security elements specific to the optional Administration Group. What follows are security elements related to these optional functions. Therefore, it is the responsibility of the Security Target Editor to include these security elements.

Security Problem Definition

Threats

T.SCC_CREDENTIAL_UNAUTHORIZED_UPDATE Unauthorized update of SCC credential

An attacker impersonates administrator to perform unauthorized update of SCC credential.

Threaten Assets: Relevant assets are [D.SCC_AUTHENTICATION_SecretKEY, D.SCC_AUTHENTICATION_PubKEY, D.SAD_KEY, D.ADMIN_RAD, D.ADMIN_VAD].

Application Note:

[ISO-29115] T.CredentialRenewal: UnauthorizedRenewal, T.CredentialRenewal:Tampering

T.SERVER_CREDENTIAL_UNAUTHORIZED_UPDATE Unauthorized update of SERVER (SAP HSM) authentication key

An attacker impersonates administrator to perform unauthorized update of SERVER (SAP HSM) authentication key to allow fake server authentication.

Threaten Assets: Relevant assets are [D.SAP_HSM_AUTHENTICATION_PubKey, D.ADMIN_RAD, D.ADMIN_VAD].

T.SCC_CREDENTIAL_DISCLOSURE Disclosure of Holder or SCC credential during update

An attacker discloses SCC credential during update performed by administrator.

Threatened assets: Relevant assets are [D.SCC_AUTHENTICATION_SecretKEY, D.SAD_KEY, D.ADMIN_RAD, D.ADMIN_VAD].

Application Note:

[ISO-29115] T.CredentialRenewal: Disclosure

T.SIGN_CREDENTIAL_UNAUTHORIZED_UPDATE Unauthorized update of Signatory credential

An attacker impersonates administrator to perform unauthorized update of Signatory or Administrator credential.

Threaten Assets: Relevant assets are [D.SIGNATORY_RAD, D.ADMIN_RAD, D.ADMIN_VAD].

Application Note:

[ISO-29115] T.CredentialRenewal: UnauthorizedRenewal, T.CredentialRenewal: Tampering

T.SIGN_CREDENTIAL_DISCLOSURE Disclosure of Signatory credential during update

An attacker discloses Signatory credential during update performed by administrator.

Threatened assets: Relevant assets are [D.SIGNATORY_RAD, D.ADMIN_RAD, D.ADMIN_VAD].

Application Note:

[ISO-29115] T.CredentialRenewal: Disclosure

Security Objectives for the TOE

OT.HOLDER_RAD_HOLDER-SIDE RAD Update in usage phase

In usage phase, only on signatory request, TOE shall be able to replace the Holder RAD stored in SCC when the administrator is authenticated. Replacement is done securely to avoid any disclosure of RAD.

OT.ADMIN_AUTHENTICATION Admin Authentication by TOE

The TOE shall provide mechanisms to authenticate Administrator. Administrator authentication shall use a RAD / VAD mechanism different for each Holder (Administrator and Issuer). The number of failed user authentication attempts shall be limited. Administrator authentication is performed securely to avoid disclosure of RAD and VAD.

OT.ADMINISTRATION Administration in usage phase

In usage phase, administrator, once it is authenticated, can perform securely administration activities relevant to SCC (as change of administrator RAD, SCC keys, SERVER authentication key(s), SAD key) only on signatory request.

Replacement is done securely to avoid any disclosure or loss of integrity of sensitive data.

Security Objectives Rationale

T.SCC_CREDENTIAL_UNAUTHORIZED_UPDATE,
T.SCC_CREDENTIAL_DISCLOSURE,
T.SERVER_CREDENTIAL_UNAUTHORIZED_UPDATE are countered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SCC_CREDENTIAL_UNAUTHORIZED_UPDATE,
T.SCC_CREDENTIAL_DISCLOSURE,
T.SERVER_CREDENTIAL_UNAUTHORIZED_UPDATE are countered by **OT.ADMINISTRATION** assuming that only administration activities relevant to SCC can be performed by authenticated administrator.

T.SCC_CREDENTIAL_UNAUTHORIZED_UPDATE is also countered by **OE.ADMINISTRATOR** assuming that issuer is trusted and well-trained, and **OE.KEY_GENERATION** assuming secure key generation and management.

T.SCC_CREDENTIAL_DISCLOSURE, T.SERVER_CREDENTIAL_DISCLOSURE are also countered by **OE.ADMINISTRATOR** assuming that administrator is trusted and well-trained, and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

T.SIGN_CREDENTIAL_UNAUTHORIZED_UPDATE is countered **OT.ADMIN_AUTHENTICATION** by assuming secure management of RAD / VAD for admin authentication done on Holder side. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGN_CREDENTIAL_UNAUTHORIZED_UPDATE is also countered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data, and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

T.SIGN_CREDENTIAL_DISCLOSURE is countered by **OT.HOLDER_RAD_HOLDER-SIDE** by assuming secure management of RAD / VAD for user authentication done on Holder side. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGN_CREDENTIAL_DISCLOSURE is also countered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data, and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.

Security Requirements

The Administration Group is covered by the following SFRs:

- FIA_ATD.1
- FIA_UAU.1
- FIA_UID.1
- FIA_USB.1
- FDP_RIP.1
- FMT_MSA.2
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMR.1
- FPT_TDC.1/SC
- FTP_ITC.1/SC
- FDP_ACC.1/RADChange
- FDP_ACF.1/RADChange
- FDP_ITC.2/RADChange
- FIA_AFL.1/ADMIN
- FMT_SMF.1/ADMIN
- FMT_MSA.1/ADMIN

FDP_ACC.1/RADChange Change RAD Subset access control

FDP_ACC.1.1/RADChange Change RAD Subset access control The TSF shall enforce the **[*assignment: access control SFP*]** on **[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]**.

The TSF shall enforce the **access control SFP during the Usage phase** on

- Subjects: **S.Command_Manager, Authorized S.Signatory**, **Authorized S.Administrator**
- Objects: **ADMIN_RAD, SIGNATORY_RAD**
- Operations: **Change**

FDP_ACF.1/RADChange Security attribute based access control

FDP_ACF.1.1/RADChange Security attribute based access control The TSF shall enforce the **[access control SFP during the Usage phase]** to objects based on the following: **[S.Signatory can**

change via S.Command_Manager the SIGNATORY_RAD, S.Administrator can change via S.Command_Manager the ADMIN_RAD and the SIGNATORY_RAD, *[assignment: others]*].

FDP_ACF.1.2/RADChange Security attribute based access control The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[only S.Signatory can change the SIGNATORY_RAD, only S.Administrator can change the ADMIN_RAD, [assignment: additional rules]**.

FDP_ACF.1.3/RADChange Security attribute based access control The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.

FDP_ACF.1.4/RADChange Security attribute based access control The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

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

FDP_ITC.2.1/RADChange Import of user data with security attributes The TSF shall enforce the **[information flow control SFP during the usage Phase]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/RADChange Import of user data with security attributes The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/RADChange Import of user data with security attributes 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/RADChange Import of user data with security attributes 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//RADChange Import of user data with security attributes The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[importation operations of Authentication user data (defined in Table 13, related to an Authorized S.Administrator during the usage Phase) through a secure communication based upon the attribute AT.SecureChannel, *[selection: none, [assignment: additional rules]]*]**.

Application Note:

It includes: **SIGNATORY_RAD**.

FIA_AFL.1/ADMIN Authentication failure handling

FIA_AFL.1.1/ADMIN Authentication failure handling The TSF shall detect when ***[selection: [assignment: positive integer number], an administrative configurable positive integer within [assignment: range of acceptable values]]*** unsuccessful authentication attempts occur related to **[authentication of the Administrator]**.

FIA_AFL.1.2/ADMIN Authentication failure handling When the defined number of unsuccessful authentication attempts has been **[met]**, the TSF shall **[block the administrator authentication process and return an error code, *[selection: none, [assignment: list of actions]]*]**.

FMT_SMF.1/ADMIN Specification of management functions

FMT_SMF.1.1 Specification of management functions The TSF shall be capable of performing the following management functions: **[modification of ADMIN_RAD and SIGNATORY_RAD, SAD Key, changing of SCC Authentication key(s), changing of Server Authentication key(s)]**.

FMT_MSA.1/ADMIN Management of security attributes

FMT_MSA.1.1/ADMIN The TSF shall enforce the **[assignment: access control SFP(s), information flow control SFP(s)]** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **[assignment: list of security attributes]** to **[S.Administrator]**.

Refer to Table 11 for the list of security attributes associated optional administration operations.

Security Requirements Rationale

OT.HOLDER_RAD_HOLDER-SIDE

This security objective is satisfied by the following SFRs which impose that the TOE will be able to replace securely the Signatory RAD stored in SCC when the Administrator is authenticated:

- FDP_ACC.1/RADChange, FDP_ACF.1/RADChange defines the RAD change access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE.
- FDP_ITC.2/RADChange allows importation of new Signatory RAD replacing previously stored RAD.
- FPT_TDC.1/SC (from core group) allows interpreting TSF data received from SERVER
- FTP_ITC.1/SC (from core group) provides a communication channel between TOE and SERVER

OT.ADMIN_AUTHENTICATION

This security objective is satisfied by the following SFRs which imposes that the TOE shall provide a RAD/VAD administrator authentication mechanism and limit the number of failed attempts:

- FIA_ATD.1 (from core group) defines the security attribute list for each authorized subject that are also used for authentication and signature mechanisms.
- FIA_UAU.1 (from core group) ensures the ability to define the list of operations allowed prior and after authentication is performed.
- FIA_UID.1 (from core group) states that the Signatory or Administrator has to be successfully identified before performing any action.
- FIA_USB.1 (from core group) requires associating the identity and the role with the subjects acting for the authenticated user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FDP_RIP.1 (from core group) ensures protection of residual information against disclosure.

- FIA_AFL.1/ADMIN ensures the ability to define the count of authentication failure attempt and to take handling actions when the defined count is reached or exceeded.

OT.ADMINISTRATION

This security objective is satisfied by the following SFRs which imposes that the Administrator once authenticated shall be able to perform securely administration activities relevant to SCC (as change of administrator RAD, SCC keys, SAD key):

- FMT_SMF.1/ADMIN requires to specify management functions, such as security attributes, TSF data and security functions, etc., to be executed by TSF.
- FMT_MSA.1/ADMIN provides the functions to restrict the ability to manage the security attributes to authorized administrator.
- FMT_MSA.2 ensures that only authorized value inside limits of TSF data and takes handling actions when the indicated limits are reached or exceeded.
- FMT_MSA.3 provides default values of security attributes applied to access control and information flow control policies. Alternative default values for these security attributes shall only be allowed for dedicated authorized roles.
- FMT_MTD.1 defines that the TOE only accepts secure values and restricts the ability to control the relevant TSF data to administrator. This SFR restricts the ability to export sensitive TSF data to dedicated roles, some sensitive user data like private authentication key is not allowed to be exported at all.
- FMT_SMR.1 ensures that the TOE maintains roles and the ability to associate user with the authorized role.

SFR Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/RADChange	(FDP_ACF.1)	FDP_ACF.1/RADChange
FDP_ACF.1/RADChange	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1//RADChange, FMT_MSA.3
FDP_ITC.2/RADChange	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1//RADChange FPT_TDC.1/SC, FTP_ITC.1/SC
FIA_AFL.1/ADMIN	(FIA_UAU.1)	FIA_UAU.1
FMT_SMF.1/ADMIN	No Dependencies	
FMT_MSA.1/ADMIN	[FDP_ACC.1, or FDP_IFC.1l] FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/RADChange FMT_SMR.1, FMT_SMF.1/ADMIN

Appendix B: Privacy Group module PP

This Appendix introduces the security elements specific to the optional Privacy Group. What follows are security elements related to these optional functions. Therefore, it is the responsibility of the Security Target Editor to include thase security elements.

Security Problem Definition

Asset

D.DTBSR_C

Data To Be Signed Representation received from SCA and transmitted to SERVER as defined in signature activation protocol.

Protection: Confidentiality (when privacy is required)

D.IDENTIFICATION_DATA_C

These data correspond to Holder and SCC identification data. These data are used to identify the signatory and SCC and then used as input in SAD computation. These data are supposed to be imported during enrolment phase and stored in the TOE.

Protection: Confidentiality (when privacy is required)

D.SIGN_REQUEST_C

This asset represents the signature request received from SCA and transmitted from SERVER.

Protection: Confidentiality (when privacy is required)

Threats

T.SIGOP_REQDATA_DISCLOSURE Signature Request Data Disclosure

Attacker obtains knowledge of the signature request and associated data in signature operation request during or after transmission to SCC to infer what the content of the signature and identity of signatory are.

Threaten Assets: Relevant assets are [D.DTBSR_C, D.IDENTIFICATION_DATA_C, D.SIGN_REQUEST_C].

Security Objectives for the TOE

OT.SIGNATORY_ID_IMPORT Signatory Identification Data Import

The TOE shall be able to securely import Signatory Identification data protecting data confidentiality.

OT.SECURE_CHANNEL_PRIV Secure channel for privacy between SERVER and TOE

The TOE shall manage a secure channel supporting confidentiality of exchange to assure privacy user data explicitly set in Privacy Group (as DTBSR_C, DENTIFICATION_DATA_C, SIGN_REQUEST_C).

Security Objectives Rationale

T.SIGOP_REQDATA_DISCLOSURE is countered by **OT.SECURE_CHANNEL_PRIV** requiring a secure channel to avoid data disclosure during transfer (for Privacy group) and **OT.SIGNATORY_ID_IMPORT** assuming confidential import of Signatory Identification data (for Privacy group). It is also covered by **OT.PROTECTION** protecting any sensitive data protected by

TOE and TSF data, against unauthorized disclosure and/or modification and by **OT.CRYPTO** implementing cryptographic functions protection data against disclosure.

T.SIGOP_REQDATA_DISCLOSURE is also countered by **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure.

Security Requirements

The Privacy Group is covered by the following SFRs:

- FDP_ACC.1/ENR
- FDP_ACF.1/ENR
- FDP_ITC.2/ENR_SIGN_PRIV
- FDP_ACC.1/SC
- FDP_ACF.1/SC
- FDP_UCT.1/SC

FDP_ITC.2/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy

- **FDP_ITC.2.1/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy** The TSF shall enforce the **[information flow control SFP during the Enrolment Phase]** when importing user data, controlled under the SFP, from outside of the TOE.

- **FDP_ITC.2.2/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy** The TSF shall use the security attributes associated with the imported user data.

- **FDP_ITC.2.3/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy** 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/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy** 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/ENR_SIGN_PRIV Data Import of user data with security attributes with privacy** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[importation operations of IDENTIFICATION_DATA_C through a secure communication based upon the attribute AT.SecureChannel, AT.Privacy*[selection: none, [assignment: additional rules]]*]**.

Security Requirements Rationale

OT.SIGNATORY_ID_IMPORT

This security objective is satisfied by the following SFRs which guarantee that the import of the SCD Identification Data is secure when privacy is required:

- FDP_ACC.1/ENR, FDP_ACF.1/ENR (from core group) define the access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE during the enrolment phase.
- FDP_ITC.2/ENR_SIGN_PRIV requires the TSF to import confidential signatory data unambiguously associated with their security attributes by an authorized

Administrator during the Enrolment Phase through a secure communication protecting confidentiality.

OT.SECURE_CHANNEL_PRIV

This security objective is satisfied by the following SFRs which impose that the TOE shall be able to create a secure channel with SERVER and to manage it to assure confidentiality of D.DTBSR_C, D.SIGN_REQUEST_C (and D.IDENTIFICATION_DATA_C if exchange) exchange to assure user data privacy:

- FDP_ACC.1/SC, FDP_ACF.1/SC (from core group) defines the secure channel access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE.
- FDP_UCT.1/SC (from core group) addresses the protection of the data containing confidential information during data exchange.

SFR Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ITC.2/ENR_SIGN_PRIV	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/ENR, FPT_TDC.1/SC, FTP_ITC.1/SC

Appendix C: HOLDER-SIDE Authentication Group module PP

This Appendix introduces the security elements specific to the HOLDER-SIDE Authentication Group. What follows are security elements related to these functions. Therefore, it is the responsibility of the Security Target Editor to include these security elements.

Security Problem Definition

Asset

D.SIGNATORY_HOLDER-SIDE

This asset, associated to the signatory role, corresponds to the reference authentication data used to perform comparison with verification authentication data in Signatory authentication security function. When biometrics is used, the signatory must be involved to be generated.

Protection: integrity and confidentiality.

D.SIGNATORY_VAD_HOLDER-SIDE

This asset, associated to the signatory role, corresponds to the verification authentication transient data generated or imported in SCC to be used in HOLDER-SIDE signatory authentication security function. When biometrics is used, the signatory must be involved to be generated.

Protection: integrity and confidentiality.

Threats

T.SIGNATORY_IMPERSONATION_HOLDER-SIDE_ENR Signatory impersonation during enrolment phase

Attacker impersonates signatory during enrolment phase:

- by obtaining credential (RAD) during generation, storage or transfer to Signatory,
- by altering or replacing Signatory credential (RAD) by data known during the credential creation process,
- by obtaining a credential that does not belong to him/her and by masquerading as the rightful entity causes the Issuer to activate the credential to allow fake authentication by attacker to SCC and then to SERVER.

Threaten Assets: Relevant assets are [D.SIGNATORY_RAD].

Application Note:

[ISO-29115] T.Impersonation, T.CredentialCreation:Tampering, T.CredentialCreation:UnauthorizedCreation, T.CredentialIssuance:Disclosure, T.CredentialStorage:Disclosure, T.CredentialStorage:Tampering, T.CredentialStorage:Duplication, T.CredentialStorage:DisclosureByEntity

T.SIGNATORY_IMPERSONATION_HOLDER-SIDE Signatory impersonation in usage phase

Attacker impersonates signatory using a genuine SCC in operational phase during authentication by SCC using several means as

- forging signatory authentication data,
- obtaining holder credential insecurely stored by issuer or Administrator,
- disclosure of VAD during transfer between Holder device and SCC,
- disclosure during comparison of VAD with RAD in SCC,

- guessing RAD with a brute force attack,
- bypassing signatory authentication process,
- reusing not yet fully revoked signatory authentication data,
- denying having used repudiated credential or weakly renewed credential to allow fake authentication by attacker to SCC and then to TW4S

Threaten Assets: Relevant assets are [D.SIGNATORY_VAD_HOLDER-SIDE, D.SIGNATORY_RAD].

Application Note:

[ISO-29115] T.Impersonation, T.CredentialStorage:Disclosure, T.CredentialStorage: Tampering, T.CredentialStorage:Duplication, T.CredentialStorage:DisclosureByEntity, T.CredentialRevocation:DelayedRevocation, T.CredentialRevocation:UseAfterDecommissioning, T.OnlineGuessing, T.OfflineGuessing, T.CredentialDuplication, T.CredentialTheft, T.SpoofingAndMasquerading

OSP.ENROLMENT_RULES_RAD_HOLDER-SIDE

The Holder enrolment for HOLDER-SIDE RAD is done using the rules conformant for LoA4 level as defined in [ISO-29115] including a secure identity proofing policy and procedure.

OSP.ENROLMENT_SECURE_PROCESS_RAD_HOLDER-SIDE

Enrolment and credential management process shall be done securely according to rules conformant for LoA4 level as defined in [ISO-29115]. It includes a secure process for HOLDER-SIDE RAD creation, issuance, storage, revocation, destruction and renewal. A record of the registration, history, and status of each credential (including revocation) shall be maintained by the CSP. The duration of retention shall be specified in the CSP policy.

Security Objectives for the TOE

OT.HOLDER_RAD_ HOLDER-SIDE_ENR HOLDER-SIDE RAD Importation during Enrolment phase

The TOE shall be able to securely import the holder HOLDER-SIDE RAD during enrolment phase when the Administrator is authenticated. Import is performed securely to avoid disclosure of RAD.

OT.USER_AUTHENTICATION_HOLDER-SIDE User Authentication by TOE

The TOE shall provide mechanisms to authenticate Holder. Signatory authentication shall use a RAD / VAD mechanism dedicated to Signatory. The number of failed user authentication attempts shall be limited. Before the user authenticates himself to the TOE, the TOE shall not deliver data that could enable the Signatory identification. Signatory authentication is performed securely to avoid disclosure of RAD and VAD.

Security Objectives Rationale

T.SIGNATORY_IMPERSONATION_HOLDER-SIDE_ENR is countered by **OT.HOLDER_RAD_HOLDER-SIDE_ENR** assuming secure import of the Signatory RAD during enrolment phase. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGNATORY_IMPERSONATION_HOLDER-SIDE is countered by **OT.USER_AUTHENTICATION_HOLDER-SIDE** assuming secure management of RAD / VAD for user authentication done on Holder side. It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGNATORY_IMPERSONATION_HOLDER-SIDE is also countered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data.

OSP.ENROLMENT_RULES_RAD_HOLDER-SIDE is covered by **OT.HOLDER_RAD_HOLDER-SIDE _ENR** assuming secure import of the Holder HOLDER-SIDE RAD.

OSP.ENROLMENT_SECURE_PROCESS_RAD_HOLDER-SIDE is covered by **OT.HOLDER_RAD_HOLDER-SIDE_ENR** assuming secure import of the Holder HOLDER-SIDE RAD during the enrolment phase.

Security Requirements

The HOLDER-SIDE Authentication Group is covered by the following SFRs:

- FIA_ATD.1
- FIA_UAU.1
- FIA_UID.1
- FIA_USB.1
- FDP_RIP.1/HOLDER-SIDE
- FIA_AFL.1/HOLDER-SIDE
- FDP_ACC.1/ ENR_RAD_ HOLDER-SIDE
- FDP_ACF.1/ ENR_RAD_HOLDER-SIDE
- FDP_ITC.2/ENR_AUTH_RAD_HOLDER-SIDE
- FMT_MSA.1/ENR_RAD_HOLDER-SIDE

FDP_RIP.1/HOLDER-SIDE Subset residual information protection

FDP_RIP.1.1/HOLDER-SIDE Subset residual information protection The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***[selection: allocation of the resource to, deallocation of the resource from, both]*** the following objects: **[D.SIGNATORY_VAD_ HOLDER-SIDE *[selection: none, [assignment: additional objects]]*]**.

FIA_AFL.1/HOLDER-SIDE Authentication failure handling

FIA_AFL.1.1/HOLDER-SIDE Authentication failure handling The TSF shall detect when ***[selection: [assignment: positive integer number], an administrative configurable positive integer within [assignment: range of acceptable values]]*** unsuccessful authentication attempts occur related to **[authentication of the Signatory]**.

FIA_AFL.1.2/HOLDER-SIDE Authentication failure handling When the defined number of unsuccessful authentication attempts has been **[met]**, the TSF shall **[block the signatory authentication process and return an error code, *[selection: none, [assignment: list of actions]]*]**.

FDP_ACC.1/ENR_RAD_HOLDER-SIDE Subset access control

FDP_ACC.1.1/ENR_RAD_HOLDER-SIDE Subset access control The TSF shall enforce the ***[assignment: access control SFP]*** on ***[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]***.

The TSF shall enforce the **access control SFP during the Enrolment phase** on

- Subjects: **S.Command_Manager, S.Communication_Manager, Authorized S.Administrator**,
- Objects: **D.SIGNATORY_RAD during the Enrolment Phase, *[selection: none, [assignment: additional objects]]***
- Operations: **All operations defined for management of D.SIGNATORY_RAD** defined **in Table 12 during the Enrolment Phase, *[selection: none, [assignment: additional operations]]***

FDP_ACF.1/ENR_RAD_HOLDER-SIDE Security attribute based access control

FDP_ACF.1.1/ENR_RAD_HOLDER-SIDE Security attribute based access control The TSF shall enforce the **[access control SFP during the Enrolment phase]** to objects based on the following: **[all operations on (during the Enrolment Phase) between subjects and D.SIGNATORY_RAD defined in Table 12 based upon the attributes defined in Table 11, *[selection: none, [assignment: additional operations]]*]**.

FDP_ACF.1.2/ENR_RAD_HOLDER-SIDE Security attribute based access control The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[all rules defined for D.SIGNATORY_RAD** management **in Table 13 and received from an authorized S.Command_Manager, S.Communication_Manager, S.Administrator during the Enrolment Phase]**.

FDP_ACF.1.3/ENR_RAD_HOLDER-SIDE Security attribute based access control The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/ENR_RAD_HOLDER-SIDE Security attribute based access control The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[all rules defined in Table 13 and received from unauthorized S.Administrator during the Enrolment Phase, *[selection: none, [assignment: additional rules]]*].**

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

FDP_ITC.2.1/ENR_AUTH_RAD_HOLDER-SIDE Import of user data with security attributes The TSF shall enforce the **[information flow control SFP during the Enrolment Phase]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/ENR_AUTH_RAD_HOLDER-SIDE Import of user data with security attributes The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/ENR_AUTH_RAD_HOLDER-SIDE Import of user data with security attributes 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/ENR_AUTH_RAD_HOLDER-SIDE Import of user data with security attributes 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/ENR_AUTH_RAD_HOLDER-SIDE Import of user data with security attributes The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[importation operations of Authentication user data (defined in Table 13, related to an Authorized S.Administrator during the Enrolment Phase) through a secure communication based upon the attribute AT.SecureChannel, *[selection: none, [assignment: additional rules]]*]**.

Application Note:

It includes: **SIGNATORY_RAD**.

FMT_MSA.1/ENR_RAD_HOLDER-SIDE Management of security attributes

FMT_MSA.1.1/ENR_RAD_HOLDER-SIDE Management of security attributes The TSF shall enforce the **[access control SFP during the Enrolment phase]** to restrict the ability to [**all operations defined in Table 12 during the Enrolment Phase, *[selection: none, [assignment: additional operations]]*]** the security attributes **[attributes defined in Table 11, *[selection: none, [assignment: additional security attributes]]*]** to **[S.Administrator, S.Command_manager, S.Communication_manager]**.

Application Note: Such requirement concerns management of security attributes for HOLDER-SIDE RAD during signatory enrolment.

Security Requirements Rationale

OT.USER_AUTHENTICATION_HOLDER-SIDE

This security objective is satisfied by the following SFRs which imposes that the TOE shall provide a RAD/VAD user authentication mechanism and limit the number of failed attempts:

- FIA_ATD.1 (from core group) defines the security attribute list for each authorized subject that are also used for authentication and signature mechanisms.
- FIA_UAU.1 (from core group) ensures the ability to define the list of operations allowed prior and after authentication is performed.
- FIA_UID.1 (from core group) states that the Signatory or Administrator has to be successfully identified before performing any action.

- FIA_USB.1 (from core group) requires associating the identity and the role with the subjects acting for the authenticated user. Also, the TSF shall enforce rules governing changes of these security attributes by the implementation of commands that perform these changes.
- FDP_RIP.1/HOLDER-SIDE ensures protection of residual information against disclosure.
- FIA_AFL.1/HOLDER-SIDE ensures the ability to define the count of authentication failure attempt and to take handling actions when the defined count is reached or exceeded.

OT.HOLDER_RAD_HOLDER-SIDE _ENR

This security objective is satisfied by the following SFRs which guarantee that the import of the Signatory HOLDER-SIDE RAD during the enrolment phase is secure:

- FDP_ACC.1/ENR_RAD_HOLDER-SIDE, FDP_ACF.1/ENR_RAD_HOLDER-SIDE define the access control policy specifying the rules to be applied to control the access to objects stored in or processed by the TOE during the enrolment phase.
- FDP_ITC.2/ENR_AUTH_RAD_HOLDER-SIDE requires the TSF to import Authentication user data and keys unambiguously associated with their security attributes by an authorized Administrator during the Enrolment Phase through a secure communication.
- FMT_MSA.1/ENR_RAD_HOLDER-SIDE ensures that the authorized subject manages security attributes applied to access control and information flow control policies during the enrolment phase.

FDP_RIP.1/ HOLDER-SIDE	OT.USER_AUTHENTICATION_HOLDER-SIDE	
FIA_AFL.1/ HOLDER-SIDE	OT.USER_AUTHENTICATION_HOLDER-SIDE	
FDP_ACC.1/ENR_RAD_HOLDER-SIDE	OT.HOLDER_RAD_HOLDER-SIDE _ENR Holder RAD Importation during Enrolment phase	
FDP_ACF.1/ENR_RAD_HOLDER-SIDE Security attribute based access control	OT.HOLDER_RAD_HOLDER-SIDE_ENR Holder RAD Importation during Enrolment phase	
FDP_ITC.2/ENR_AUTH_RAD_HOLDER-SIDE Import of user data without security attributes	OT.HOLDER_RAD_HOLDER-SIDE_ENR Holder RAD Importation during Enrolment phase	
FMT_MSA.1/ENR_RAD_HOLDER-SIDE Management of security attributes	OT.HOLDER_RAD_HOLDER-SIDE_ENR Holder RAD Importation during Enrolment phase	

SFR Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FIA_AFL.1/HOLDER-SIDE	(FIA_UAU.1)	FIA_UAU.1
FDP_RIP.1/HOLDER-SIDE	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/ENR_RAD_HOLDER-SIDE	(FDP_ACF.1)	FDP_ACF.1/ENR_RAD_HOLDER-SIDE
FDP_ACF.1/ENR_RAD_HOLDER-SIDE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ENR_RAD_HOLDER-SIDE , FMT_MSA.3/SC
FDP_ITC.2/ENR_AUTH_RAD_HOLDER-SIDE	FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/ENR_RAD_HOLDER-SIDE , see rationale §7.3.3.1.1, see rationale §7.3.3.1.1
FMT_MSA.1/ENR_RAD_HOLDER-SIDE	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ENR_RAD_HOLDER-SIDE , FMT_SMF.1 FMT_SMR.1

Appendix D: SERVER-SIDE Authentication Group module PP

This Appendix introduces the security elements specific to the SERVER-SIDE Authentication Group. What follows are security elements related to these functions. Therefore, it is the responsibility of the Security Target editor to include these security elements.

Security Problem Definition

Asset

D.SIGNATORY_VAD_SERVER-SIDE

This asset, associated to the signatory role, corresponds to the verification authentication transient data transfer to TSCM to be used in remote signatory authentication security function. When biometrics is used, the signatory must be involved to be generated.

Protection: integrity and confidentiality.

Threats

T.SIGNATORY_IMPERSONATION_SERVER-SIDE Signatory impersonation in usage phase

Attacker impersonates signatory using a genuine SCC during authentication by TW4S in operational phase using several means as

- forging signatory authentication data,
- disclosure of VAD during transfer between Holder device and TW4S,
- bypassing signatory authentication process,
- reusing not yet fully revoked signatory authentication data,
- denying having used repudiated credential or weakly renewed credential to allow fake authentication by attacker to SCC and then to TW4S.

Threaten Assets: Relevant assets are [D.SIGNATORY_VAD_SERVER-SIDE].

Application Note:

[ISO-29115] T.Impersonation, T.CredentialStorage:Disclosure, T.CredentialStorage: Tampering, T.CredentialStorage:Duplication, T.CredentialStorage:DisclosureByEntity, T.CredentialRevocation:DelayedRevocation, T.CredentialRevocation:UseAfterDecommissioning, T.OnlineGuessing, T.OfflineGuessing, T.CredentialDuplication, T.CredentialTheft, T.SpoofingAndMasquerading, T.Eavesdropping

Security Objectives for the TOE

OT.USER_AUTHENTICATION_SERVER-SIDE Contribution of TOE to User Authentication done remotely

The TOE shall provide mechanisms to contribute to the user authentication when it is done remotely. TOE shall import and securely transfer VAD to TSCM and receives answer from SERVER demonstrating user authentication has been performed as defined in SAP. Such status will be used to authorize SAD computation by TOE.

Application note: Status of SERVER answer will impact TOE ability to compute a SAD.

Security Objectives Rationale

T.SIGNATORY_IMPERSONATION_SERVER-SIDE is countered by **OT.SECURE_CHANNEL** requiring a secure channel to avoid data disclosure during transfer and by **OT.USER_AUTHENTICATION_SERVER-SIDE** assuming secure management and transfer of

VAD for user authentication done remotely (for SERVER-SIDE Authentication group). It is also covered by **OT.PROTECTION** protecting any sensitive data protected by TOE and TSF data, against unauthorized disclosure and/or modification.

T.SIGNATORY_IMPERSONATION_SERVER-SIDE is also countered by **OE.HOLDER** avoiding impersonation by keeping confidentiality of its authentication data and **OE.SECURE_COPY** assuming secure management of sensitive data in operational phase avoiding unauthorized use during enrolment phase.
T.SIGNATORY_IMPERSONATION_SERVER-SIDE is also countered by **OE.CRYPTO** requiring platform implements cryptographic functions protection data against disclosure.

Security Requirements

- **FDP_RIP.1/SERVER-SIDE Subset residual information protection**

FDP_RIP.1.1/SERVER-SIDE Subset residual information protection The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***[selection: allocation of the resource to, deallocation of the resource from, both]*** the following objects: **[D.SIGNATORY_VAD_SERVER-SIDE *[selection: none, [assignment: additional objects]]*]**.

The Remote Authentication Group is covered by the following SFRs:

- FIA_ATD.1
- FDP_UCT.1/SC
- FDP_UIT.1/SC
- FDP_RIP.1/SERVER-SIDE

Security Requirements Rationale

OT.USER_AUTHENTICATION_SERVER-SIDE

This security objective is satisfied by the following SFRs which imposes that the TOE shall contribute to the Holder authentication by importing and securely transfer VAD to SERVER and receives answer:

- FIA_ATD.1 (from core group) defines the security attribute list for each authorized subject that are also used for authentication and signature mechanisms.
- FDP_UCT.1/SC (from core group) securely transfer VAD to SERVER keeping its confidentiality
- FDP_UIT.1/SC (from core group) securely transfer VAD to SERVER and result of authentication by SERVER keeping their integrity.
- FDP_RIP.1/SERVER-SIDE ensures protection of residual information against disclosure.

SFR Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FDP_RIP.1/SERVER-SIDE	No Dependencies	