Protection Profile for

Trusted Signature Creation Module in TW4S

Publication date	**:**	19 February 2016
Reference	**:**	PP-RSCD-TSCM/TW4S
Version	**:**	1.2

Table of Content

List of figures

List of tables

1 PP Introduction

1.1 PP reference

Title	Protection Profile for - Trusted Signature Creation Module in TW4S
Reference	PP-RSCD-TSCM/TW4S
Version	1.2
Sponsor	ANSSI
CC version	3.1 revision 4
Assurance level	The minimum assurance level for this PP is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General status	Final draft
Key words	EIDAS, qualified signature creation device, remote signature creation device

1.2 Protection Profile Overview

This Protection Profile (PP) defines the security requirements of a Trustworthy Signature Creation Module (TSCM) used by TSP as part of their infrastructure for Trustworthy System Supporting Server Signing (TW4S) that generates advanced electronic signatures as defined in Regulation (EU) N°910/2014 [17].

The TSP implementing TW4S will operate a Server Signing Application (SSA) 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 419 241 [EN-419241-1].

In order to allow to evaluate the conformity of the SSA with the requirements of article 29 and Annex II of Regulation (EU) N°910/2014 to generate a qualified electronic signature, this document and the document [PP SAP] defines respectively a TSCM and a SCC component that must work together to function as a Remote Qualified Signature Creation Device. The architecture in which they operate consists of:

- A Signature Creation Application (SCA),
- A Single Control Component (SCC),
- A Trustworthy Signature Creation Module (TSCM),
- A Hardware Security Module (HSM) including a local application (named SAP HSM) and used by the TSCM to protect the user key and ensure the security of most critical operations.

The SCC, the TSCM and the HSM work in combination to ensure that the Signature Activation Protocol (SAP) is used to transmit the signature request and the Signature Activation Data (SAD). The signature creation data (SCD) of the signatory is operated inside the HSM module. This process ensures that the user's SCD can be activated for signature operations only after validation by the signatory using his SCC. The SSA may include additional components but they shall not enforce the security of the signature operation, and they shall not be able to interfere into the operation of the evaluated components.

This Protection Profile specifies the security requirements for the TSCM.

A TSCM component might in practice provide additional functionalities to those described in this document. In this case, the security target for the product will be completed to describe the security requirements for those added functionalities, in addition to conforming to the security requirements described in this Protection Profile.

2 TOE Overview

2.1 System overview

The protection profile defines the security objectives and requirements for a Trustworthy Signature Creation Module (TSCM) which provides service allowing the private key of a signatory to be remotely used to sign cryptographic documents while staying under his sole control, ensured by the fact that only the Single Control Component (SCC) that the signatory owns and that has been associated with his private key will allow the activation of the key for signature operation. The combination of the TSCM and of the SCC is the Remote Qualified Signature Creation Device (RQSCD) as defined by the regulation [REGULATION]

The TOE relies on a Cryptographic Module for Trust Services as defined by [PP SAP HSM] allowing signature operation activation, SCC authentication and ciphered key retrieving (optional).

The TOE is part of a TW4S system as shown in the next figure. The TW4S operates on a networked server in order to allow users to connect for signature from various local environments.

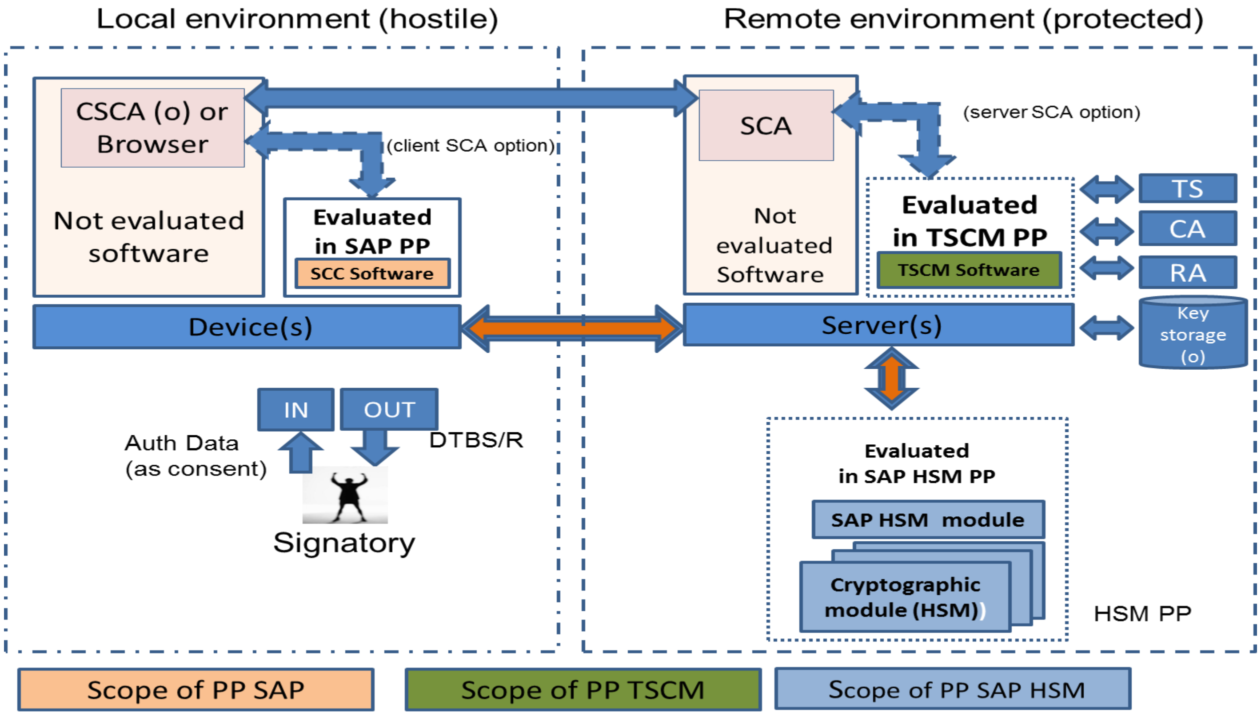

Figure 1: System overview and TSCM scope

Due to the generic definition of the TOE in this PP, the particular hardware/software/firmware required by the TOE is not defined by this PP.

Because some TOE functionalities are optional, or may be realized in different ways to obtain the same security level, optional threats/objectives/SFRs packages have been defined in module-PP available in the appendix of this document.

The whole system that includes the TSCM component covers the same threats that the SSCD, defined in [PP SSCD] but the remote signature introduces additional threats described in this PP. The solution must provide solutions to assure that exchanges coming directly from the signatory or information collected about him by the personalisation agent can be transmitted to the remote system without compromising its integrity or its confidentiality. Furthermore, one RSCD system will handle the keys of many signatories, and must therefore provide means to assure perfect isolation between the signatories' data.

2.2 TOE Type

The Target of Evaluation (TOE) is the Trusted Signature Creation Module comprising software that is part of a system performing secure remote creation of electronic signature. The security requirements for the solution incorporated all requirements of the regulation [REGULATION] on electronic identification and trust services for electronic transactions in the internal market.

The TOE comprises at least the software implementing the TSCM features, described in this document, and its associated guidance documentation.

2.3 TOE life cycle

The TOE life cycle consists of a succession of cycle phases including stages for development, production, preparation and operational use.

Phase 1 "Development"

The TOE developer develops the TOE application and its guidance documentation using any appropriate guidance documentation for components working with the TOE, including the SAP HSM module.

Phase 2 "Delivery"

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

Phase 3 "Installation and configuration"

The TSP installs and configures the TOE with the appropriate configuration and initialisation data. Installation may allow creating the Administrator accounts.

Phase 4 "Operational phase"

In operation, the TOE can be used by Administrators to create Auditor and Personalisation Agent accounts. The Personalisation Agent may create signatory User accounts. User account dedicated to signatory can be used for signature request on behalf of signatory. Each user account separately may reach end of life while the TOE itself is still in operational phase.

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

2.4 Signatory account life cycle

The steps of the life cycle of each signatory account are the following:

1. Creation and initialization of the account, including enrolment for authentication and signature service
2. Generation of the certificate
3. Activation of signature service
4. Use of signature service
5. Deactivation of signature service
6. Lock and/or Destruction of the account

Phase 1 "Creation and initialisation"

(Step1) The personalisation of the signatory account includes (i) the survey of the signatory, (ii) the enrolment of the Signatory RAD (in case of remote authentication), and (iii) the configuration of the

TOE. The personalisation is performed by the Personalisation Agent injecting the authenticated data to the TOE for integration into the TOE configuration.

(Step2) The Certificate Generation Application (CGA) generates the signatory certificate using the information provided by the TOE.

(Step3) The account is then activated, either by direct activation on the TOE, or by activation of the SCC.

Application note:

Different deployment scenarios may exist depending on whether the signatory already owns his SCC, or not. When a dedicated SCC device is used, it can be initialized and personalised in advance, and kept inactivated until its delivery to the user. The activation of the account may then consist in the activation of the SCC after delivery. When a SCC device not dedicated for this service is used, the personalisation requires the presence of the signatory and the presentation of his SCC.

The personalisation phase depends on TSP-specific security requirements. Production, configuration and initialisation procedures will be analysed during both the SCC evaluation and the TSCM evaluation insofar as the interaction with the TSCM ensures that the procedure is correctly and safely pursued.

Phase 2 “Operational Use”

(Step4) The TOE is used by the Signatory to create signature using his SCC and the SCA.

Phase 3 “Deactivation and End of life”

(Step5) Deactivation of the user account blocks any signature operation. The account may still be reactivated.

(Step6) The destruction of the user account shall ensure that the SCD cannot be anymore activated.

2.5 Users

This protection profile considers following users (human or IT entity possibly interacting with the TOE from outside of the TOE boundary).

Signatory

The *Signatory* is the authorized user of the system for whom the issuing State or Organization created the SCD and associated it with a certificate. While this PP describes the operation of the system when used by a single signatory, multiple signatories can use the TOE simultaneously to realize signature operations.

Administrator

The *Administrator* is in charge of handling the IT system in which the TOE is operating and ensuring its security and proper operation. He performs the TOE initialisation, the TOE personalisation, the TOE user management, and other TOE administrative functions.

Personalisation Agent

The *Personalisation Agent* is acting on behalf of the issuing Organization to enrol the signatory by some or all of the following activities (i) establishing the identity of the signatory for the identification data included in the certificate, (ii) providing this data to the TOE ensuring it’s integrity (iii) initiating the lifecycle of the signatory account on the TOE.

Auditor

The *Auditor* is in charge of performing the TOE audit functions.

Signature Creation Application

The *Signature Creation Application* is the application that creates electronic signatures, sending a DTBS/R to the TOE, and integrating in the electronic signature the signature result returned by the TOE. The SCA also ensures that the communication with the TOE is safe and uncompromised and therefore protects the signatory against any threat by an attacker on the communication channel with the TOE.

Sole Control Component

The *Sole Control Component* is the device used by the signatory to authenticate itself to the TOE in order to approve the activation of his key for the signature of a specific data object. The SCC also ensures that the communication with the TOE is safe and therefore protects the signatory against the attacks on the communication channel between the SCC and the TOE.

2.6 TOE usage and security features for operational use

The main functionality of the TOE is to enable the Signatory to realize signature operation using his SCD after authentication. The TOE also provides the server part of the signature activation protocol (SAP) that assures the sole control of the signature key.

The TOE also provides administration and audit log record features.

2.6.1 PP configurations

This protection profile is a modular PP as defined in [5]. 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:

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

Module-PP Name	Type	Description
HOLDER-SIDE AUTHENTICATION module	Alternative	This module includes all functions that are required when the Signatory authentication is done by the SCC.
SERVER-SIDE AUTHENTICATION module	Alternative	This module includes all functions that are required when the Signatory authentication is done by the SAP HSM.
PRIVACY module	Optional	This module includes the functions that assure the signatory privacy. Privacy is assured by protection of the confidentiality of sensitive data linked to the DTBS and to the signatory identity.
EXTERNAL KEY STORAGE module	Optional	This module includes all functions that are required when the signatories' keys are stored, when not used, out of the HSM.

Table 1 – Module-PP names and types

2.6.2 Signature workflow

The remote signature operation can be summarized in the following steps:

1. **Signature request**: the SCA application prepares the data necessary for the signature (DTBS/R, signatory identity, SCD id) and transfers them to the TSCM directly or through the SCC.
2. **TSCM-SCC secure channel**: A secure channel is created between the TSCM and the SCC relying on network utilities provided by the underlying systems (the Server for the TSCM and the user device for the SCC).
3. **Signatory authentication**: the signatory is authenticated in order to open his account and to access his data. Two options are available here: either the signatory is authenticated by the SCC (see HOLDER-SIDE AUTHENTICATION module), or the signatory is authenticated by the HSM (see SERVER-SIDE AUTHENTICATION module):
   a. When the signatory is authenticated by the SCC and if the signatory is successfully authenticated, the SCC can process the next steps.
   b. When the signatory is authenticated by the HSM and if the signatory is successfully authenticated, the authentication confirmation is sent to the SCC in order to process the next steps.
4. **Data transfer**: the TSCM transfers to the SCC all the data required for the SAD computation: DTBS/R, signatory identity, SCD id.
5. **SAD computation**: the signatory being authenticated, the SCC can compute the SAD using the data sent by the TSCM.
6. **SAD transfer**: the SCC sends the SAD to the SAD HSM through the SCC-TSCM secure channel.
7. **SAD verification**: the SAD HSM verifies the SAD prior to allow SCD activation for signature operation
8. **SCD activation**: after the successful SAD verification, the SAD HSM activates the SCD necessary for the signature operation. Note: when the SCD if stored outside the HSM, the TSCM has to restore the SCD in the SAD HSM before its activation.
9. **Signature**: the HSM performs the signature of the DTBS/R using the active SCD. A SAD only allows the signature of the DTBS/R used to generate that SAD.
10. **SCD deactivation**: after a signature or a set of signature, the SCD is deactivated.
11. **Signature result transfer**: the result of the signature operation is transferred from the HSM to the TSM and to the SCA application.

2.6.3 Security functions

The next paragraphs list the security functions provided by the TOE in the base-PP configuration. TOE functions specific to other configurations are described in the appendix.

2.6.3.1 Signatory and SCC enrolment (signatory account creation)

Signatory ID importation

The TOE allows importation of the Signatory identifier.

Signatory keys and certificate generation request

The TOE requests the generation of the Signatory keys to the HSM. The SVD and a Certificate Signature Request (CSR) is provided by the HSM to the TOE for the generation of the associate certificate. Then TOE requests the certificate to the CGA using SVD and CSR for the associated signatory identity.

SCC authentication key import

The TOE is able to import the SCC public key to support the SCC authentication.

2.6.3.2 SCC secure channel management

SCC authentication by the TOE

The TOE authenticates the SCC using its public key. This authentication protects against the use of fake SCC.

2.6.3.3 Server-side Signature Activation Protocol (SAP) management

The TOE ensures that the steps of the SAP protocol are properly executed at the server side. The TOE does not allow signature operations without the verification of the SAP conditions.

If the SCD is stored externally, the SCD has to be restored in the HSM prior the SCD activation.

2.6.3.4 Signature operations

After the successful completion of SAP conditions verification, the TOE transfers the signature request to the SAP HSM. The signature operation is performed by the SAP HSM, the result is received by the TOE then transferred to the SCA application.

2.6.3.5 Authentication and access control

Privileges users' authentication

The TOE authenticates the users with privileges: the Administrator, the Personalisation Agent and the Auditor.

Access control to security functions

The TOE controls the access to security functions and restricts the access to authenticated users. Authenticated users only have access to functions accessible to their role.

Role management

The TOE allows the authorized Administrator to manage the users' accounts and the users' roles.

2.6.3.6 Audit trail

The TOE creates logs and audit trail for all TOE operations and provides means to audit logs only by authorized Auditors.

3 Conformance Claims

3.1 CC Conformance Claim

This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, [1] (Part 1 strict conformance claim)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012, [2] (Part 2 extended conformance claim)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012, [3] (Part 3 strict conformance claim)
- And, the CC and CEM addenda: Modular PP, CCMB-2014-03-001, March 2014 [5]

3.2 PP Claim

This PP does not claim conformance to any other PP.

3.3 Package Claim

This PP is conforming to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

3.4 Conformance rationale

This PP does not provide a conformance rationale because it does not claim conformance to any other PP.

3.5 Conformance statement

This PP requires strict conformance (as defined in [1]) of any ST or PP, which claims conformance to this PP.

A Security Target shall claim conformity to a PP-configuration that combines the requirements from the base PP and the requirements from the PP-modules available in appendix of this document. See [5] for more details on conformance with modular PPs.

4 Security Problem Definition

The writer of a security target claiming conformance to this PP shall take care of selecting the adequate optional module-PP from the appropriate appendix at the end of this document, and complement the security problem definition with the elements extracted from the appendix.

Only the elements from the base-PP are described here.

4.1 Assets

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

4.1.1 Assets to be protected by the TOE

4.1.1.1 Signatory assets

D.IDENTIFICATION_DATA_I

These data correspond to Signatory and SCC identification data (SCC_ID). These data are used to identify the signatory and his SCC and are used as an input for SAD computation. These data are supposed to be imported during the enrolment phase and are stored in the TOE. These data also include a link between the identity of the signatory and the SCC.

Protection: integrity

D.SCC_AUTHENTICATION_KEY

These data correspond to the public key of the SCC used to authenticate the SCC associated to the signatory.

Protection: integrity

D.SIGNATORY_DATA

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

Protection: integrity and confidentiality

D.SCD

The SCD is the private key used to perform the electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD shall be maintained.

Protection: integrity and confidentiality

D.SVD

The SVD is the public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when exported by the TOE shall be maintained.

Protection: integrity

4.1.1.2 Signature operations assets

D.SIGN_REQUEST

This asset is the set of data representing the signature request of the signatory, received from the SCA.

Protection: integrity

D.DTBSR

The Data to Be Signed Representation is a set of data, or its representation, which the signatory intends to sign as generated by the SCA. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained.

Protection: integrity

D.SIGNATURE

This asset is the set of data obtained as result of signature operation performed by the SAP HSM on behalf of the signatory.

Protection: integrity

4.1.2 Sensitive assets of the TOE

D.TSCM_AUTHENTICATION_PRIVATE_KEY

This asset is the TSCM private key used to authenticate the TOE. This private key (with its associated public key) 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 operation domains.

D.TSCM_AUTHENTICATION_PUBLIC_KEY

This asset is the TSCM public key. This key is provided by the TOE to allow the its authentication when needed. This public key (with its associated private key) may be generated outside of the TOE and imported in the TOE or generated inside the TOE. The public key shall remain consistent with its corresponding private key until it is securely delivered to the CGA for certificate generation.

Protection: integrity.

D.ADMIN_RAD

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

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 during the Administrator authentication.

Protection: integrity and confidentiality.

D.PA_RAD

This asset, associated to the personalisation agent role, corresponds to the reference authentication data used to perform comparison with verification authentication data during the Personalisation Agent authentication.

Protection: integrity and confidentiality.

D.PA_VAD

This asset, associated to the personalisation agent role, corresponds to the verification authentication data generated or imported to be used during the Personalisation Agent authentication.

Protection: integrity and confidentiality.

D.AUDITOR_RAD

This asset, associated to the auditor role, corresponds to the reference authentication data used to perform comparison with verification authentication data during the Auditor authentication.

Protection: integrity and confidentiality.

D.AUDITOR_VAD

This asset, associated to the auditor role, corresponds to the verification authentication data generated or imported to be used during the Auditor authentication.

Protection: integrity and confidentiality.

D.AUDIT_DATA

This asset corresponds to the internal audit records.

Protection: integrity

4.2 Assumptions

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

A.TSP Trusted Service Provider

The TOE is hosted by a Trusted Service Provider which applies applicable procedures for its operation, and operates according to the requirements laid down in [EN319401] and [EN319431] or equivalent.

A.TSP is directly addressed by OE.TSP.

A.SECENV Secure environment

The TOE operates in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment is maintained by Administrators in a secure state.

A.SECENV is directly addressed by OE.SECENV.

A.CGA Trustworthy certificate generation application

The CGA protects the authenticity of the signatory’s name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP. It implements a set of practices in conformity with its CP/CPS which conforms to [EN319401] and [EN319411] or equivalent.

A.CGA establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.SCA Trustworthy signature creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data that the signatory wishes to sign in a form appropriate for signing by the TOE.

A.SCA establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.SCC Certified sole control component

The SCC component is certified conform to [PP SAP] and is in possession of its legitimate user.

A.SCC is directly addressed by OE.SCC.

A.SAP_HSM Certified hardware security module

The HSM module is certified conform to [PP SAP HSM].

A.SAP_HSM is directly addressed by OE.SAP_HSM.

A.AUDIT_REVIEW Audit review

It is assumed that the Auditors check the audit trails on a regular basis, and notify the corresponding authority in the case that any security incident occurred.

A.AUDIT_REVIEW is directly covered by OE.AUDIT_REVIEW.

4.3 Threats

This section describes the threats to be countered by the TOE independently or in collaboration with its operational environment.

4.3.1 Threat agents

Potential attackers of the TOE are:

- attackers having access to the communication path between the signatory local environment and the TOE,
- malicious registered signatories trying to use their privileges to sign using SCD from another registered signatory,
- malicious users (Personalisation Agent, Administrator, Auditor) intending to access data and functions for which they do not have legitimate access rights. In particular, nobody except the signatory should have access to the signatory SCD or should succeed to perform a signature on behalf of the signatory
- applications installed on the server hosting the TOE that intend to impersonate the signatory or to gain access to signatory’s sensitive data.

It is assumed that all these potential attackers have got a high attack potential.

4.3.2 Threats on enrolment

T.UNAUTHORIZED_PERSONALISATION Personalisation agent impersonation

An attacker impersonates the Personalisation Agent to perform unauthorized creation of user accounts. It may lead to unauthorized creation of SCD /SVD associated to a valid signatory or unauthorized link of valid SCD /SVD to non-accurate signatory.

T. UNAUTHORIZED_PERSONNALISATION is countered by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL requiring the personalisation agent to be authenticated before granting access to the personalisation functions. OT.AUDIT requires recording personalisation operation and OE.AUDIT_REVIEW ensures that the auditor verifies the personalisation operations logs.

T.SCC_IMPERSONATION_ENR SCC impersonation during the signatory enrolment

An attacker impersonates the SCC by making it so that a modified or fake SCC is used in enrolment phase:

- using a genuine SCC with fake or disclosed SCC authentication data

- using a fake SCC with disclosed authentication data of a genuine SCC to allow fake authentication by attacker to the TOE to be exploited in operational phase.

> *T.SCC_IMPERSONATION_ENR is countered by OT.SCC_KEY_ENR ensuring a secure enrolment process and OE.SCC ensuring that the SCC is a trustworthy SCC implementing all security features to avoid authentication data disclosure.*

4.3.3 Threats on SCC authentication & secure channel

T.SCC_IMPERSONATION SCC impersonation during the operational phase

An attacker impersonates the SCC owned by the Signatory:

- by forgering the SCC authentication data (SCC private key, SCC certificate including SCC public key),
- by obtaining the SCC authentication data (SCC private key) stored in SCC or during its usage,
- by exploiting a weakness in the authentication protocol.

> *T.SCC_IMPERSONATION is countered by OT.SCC_AUTHENTICATION ensuring that the SCC is securely authenticated by the TOE and OE.SCC ensuring the confidentiality of the SCC authentication data.*

T.SCC_TSCM_MANINTHEMIDDLE SCC-TSCM man-in-the-middle

An attacker intercepts and alters messages (containing user data and/or authentication protocol data) exchanged between the TOE and the SCC. The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the TSCM. 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 TSCM using method as:

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

By this way, the attacker replaces genuine data (signature request, DTBSR and associated SAD) by fake data during transfer between the SCC and the TSCM leading to unauthorized signature operation activation.

This threat matches with the [ISO-29115] threat T.ManInTheMiddle.

> *T.SCC_TSCM_MANINTHEMIDDLE is countered by OT.TSCM_AUTHENTICATION and OT.SCC_AUTHENTICATION ensuring a mutual authentication between the TSCM and the SCC and by OE.SECURE_CHANNEL ensuring that a secure communication path is used.*

4.3.4 Threats on signature operations

T.ILLICIT_REQUEST Unauthorized signature request

An attacker transmits to TCSM or builds on TSCM fake or improper signature requests using fake DTBS/R, on behalf of inconsistent signatory or invalid SCD.

> *T.ILLICIT_REQUEST is countered by OT.REQUEST_AUTHENTICATION that requires the authentication of the requests by the TOE.*

T.UNAUTHORIZED_SIGNATURE_ACTIVATION Unauthorized activation of the signature-creation function of the TOE

An attacker alters configuration data or the signature workflow in order to transfer the signature request to the SAP HSM without SAP conditions fulfilment. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

This threat matches with the threat SigF_Misuse for a SSCD.

> *T.UNAUTHORIZED_SIGNATURE_ACTIVATION is countered by OT.GET_SIGNATORY_AUTHENTICATION (in HOLDER-SIDE AUTHENTICATION configuration) or OT.TSCM_SIGNATORY_AUTHENTICATION (in SERVER-SIDE AUTHENTICATION configuration) that requires the authentication of the signatory. OT.SIGNATURE_ACTIVATION_PROTECTION ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.SIGNATORY ensures also that the signatory keeps their VAD confidential.*

T.DTBS_Forgery Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory approved to sign.

> *The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.*

T.SCD_Derive Derive the signature creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

> *T.SCD_Derive is countered by OT.SCD/SVD_Auth_Gen that requires a cryptographically secure generation of the SCD/SVD pair. OT.CM_SECURE_CRYPTO requires the use of a secure cryptographic module (OE.SAP_HSM) and OE.CRYPTO requires the use of secure algorithms.*

T.SVD_Forgery Forgery of the signature verification data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory prior certificate generation

> *T.SVD_Forgery is countered by OT.CM_SECURE_CRYPTO, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.*

T.Sig_Forgery Forgery of the electronic signature

An attacker forges the result of the signature operation (D.SIGNATURE), maybe using an electronic signature which has been previously created by the TOE, and the violation of the integrity of D.SIGNATURE is not detectable by verification performed by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

> *T.Sig_Forgery is countered by OT.CM_SECURE_CRYPTO and OE.CGA_QCert. OT.CM_SECURE_CRYPTO ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OE.CGA_QCert prevents forgery of*

the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

4.3.5 Threats on administration & audit

T.PRIVILEGE_ESCALATION

An attacker with a legitimate role tries to change his role in the TOE (directly or using a malicious application installed in the server) and to perform unauthorized operation for its initial role.

> *T.ROLE_MODIFICATION is countered by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL guaranteeing that only the administrator has control over the configuration of roles. OE.HOST_REVIEW requires to review regularly the configuration of the hosting platform to detect the presence of uncontrolled applications. OT.AUDIT records changes to the configuration and OE.AUDIT_REVIEW ensures that the auditor verifies the configuration changes.*

T.AUDIT_ALTERATION Illicit modification of audit data

An attacker alters the audit data of the TOE in order to hide unauthorized operations he has done on the platform.

> *T.AUDIT_ALTERATION is countered by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL requiring the auditors to be authenticated before granting access to the audit data.*

4.4 Organizational Security Policies

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

OSP.Personalisation Personalisation by the TSP

The TSP guarantees the correctness of the identity data with respect to the signatory. The personalisation of the signatory account is performed by a personalisation agent authorized by the TSP only. The personalisation is done using the rules conformant for LoA4 level as defined in [NR6] including a secure identity proofing policy and procedure.

> *OSP.Personalisation is addressed by OT.SCC_KEY_ENR, OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL requiring that only authorized personalisation agents can perform personalisation.*

OSP.TSP_Sigy_Policy Application of the appropriate policy by the TSP

The TSP shall operate the service in conformance with a signature generation service provider policy which is implemented according to the requirement of [EN 319 401] and [EN 319 431] or equivalent. All operations and operational procedures shall be realized in conformity with the requirements of the policy.

> *OSP.TSP_Sigy_Policy is addressed by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL ensuring that the configuration is under the control of the administrator configuring parameters that conform to the policy. OT.AUDIT ensures that events are audited and provided the necessary level of traceability for conformance to the policy.*

OSP.CSP_QCert Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate for the SVD exported by the TOE. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

OSP.CSP_QCert is addressed by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL ensuring that only trusted administrator can configure the product to use an appropriate CGA and OT.QCert_Request restricting the users able to request a certificate. It is also addressed by OE.CGA_QCert generating a qualified certificate.

OSP.QSign Qualified electronic signatures

The TOE is part of a signature creation system that the signatory uses to sign data with an advanced electronic signature, which is a qualified electronic signature if it is based on a valid qualified certificate. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the qualified RSCD. The qualified RSCD creates the electronic signature created with a SCD implemented in the RSCD that the signatory can maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

OSP.QSign is addressed by OT.SIGNATURE_ACTIVATION_PROTECTION and OT.CM_SECURE_CRYPTO guaranteeing that the signatory is correctly identified and has sole control over his SCD. It is also addressed by OE.CGA_QCert generating a qualified certificate.

OSP.Sigy_RSCD TOE as qualified remote signature creation device

The TOE meets the requirements for a QSCD laid down in Annex II of the regulation [1]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

OSP.Sigy_RSCD is addressed by OT.SIGNATURE_ACTIVATION_PROTECTION guaranteeing that the signatory is correctly identified and has sole control over his SCD. OT.CM_SECURE_CRYPTO requires the use of a secure cryptographic module (OE.SAP_HSM) and OE.CRYPTO requires the use of secure algorithms.

OSP.Sig_Non-Repud Non-repudiation of signatures

The lifecycle of the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

OSP.Sig_Non-Repud is addressed by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE. OT.SIGNATURE_ACTIVATION_PROTECTION guarantees that the user is correctly identified and has sole control over his SCD. OT.CM_SECURE_CRYPTO requires the use of a secure cryptographic module (OE.SAP_HSM) and OE.CRYPTO requires the use of secure algorithms. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory.

5 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

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 Security objectives on enrolment

OT.SCC_KEY_ENR SCC secure enrolment

The TOE shall securely import the data associated to the SCC, including its public key and ID during the signatory account personalisation by the Personalisation Agent.

> *The objective is provided by FDP_ITC.2/ENR that requires the secure import of the SCC data and FDP_ACC.1/ENR and FDP_ACF.1/ENR that require access control on the enrolment operations. FMT_MSA.1/ENR and FMT_MSA.3/ENR restrict the signatory account management to personalisation agents. FPT_TDC.1/ENR requires the TOE to be able to interpret the data sent by the SCC.*

OT.SCD/SVD_Auth_Gen Authorized SCD/SVD generation

The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

Authorised users include:

- The personalisation agent during the creation of a new account,
- The signatory when the TOE allows generation of new SCD/SVD pair for an existing account.

> *FDP_ACC.1/ENR and FDP_ACF.1/ENR provide access control for the signatory account management including SCD/SVD generation.*

OT.QCert_Request Authorized certificate request

The TOE shall provide security features to ensure that authorised users only may request the generation of a qualified certificated to the CGA.

Authorised users include:

- The personalisation agent during the creation of a new account,
- The signatory when the TOE allows generation of new SCD/SVD pair for an existing account.

> *FDP_ACC.1/ENR and FDP_ACF.1/ENR provide access control for the signatory account management including certificate request. FCO_NRO.2/CSR requires the signature of the certificate requests.*

5.1.2 Security objectives on SCC authentication

OT_TSCM_AUTHENTICATION TSCM authentication data

The TOE shall be able provide information to ensure its authentication.

> *FIA_API requires the TOE to provide mechanisms to external entities to authenticate the TOE.*

OT.SCC_AUTHENTICATION Authentication of the SCC

The TOE shall authenticate the SCC.

> *The objective is provided by FIA_UAU.2/SCC and FIA_UID.2/SCC that require the identification and the authentication of the SCC.*

5.1.3 Security objectives on signature operations

OT.REQUEST_AUTHENTICATION

The TOE shall authenticate the origin of the signature request.

Application Note:

The signature request can be received from the SCA directly of can be transmitted through the SCC.

> *The objective is provided by FIA_UAU.2/REQUEST and FIA_UID.2/REQUEST that require the identification and the authentication of the origin of the request.*

OT.SIGNATURE_ACTIVATION_PROTECTION Protection of the signature creation function

The TOE shall also be protected against processing any unauthorized signature request. This protection is based on a signature activation protocol (SAP) that avoids any bypass of security controls. The TOE thus shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against its use by the others.

This objective matches with the objective OT.Sigy_SigF for the SSCD.

> *The objective is provided by FDP_ACC.1/SIGNATURE and FDP_ACF.1/SIGNATURE that require the SAP protocol to be successful before to allow signature operations only to the legitimate signatory.*

OT.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

> *The objective is provided by FDP_SDI.2/DTBSR that requires that the DTBS/R has not been altered by the TOE*

OT.CM_SECURE_CRYPTO

The TOE shall use the SAP HSM module for all cryptographic operations, using only approved algorithms and algorithm parameters, as well as security functions that properly link security parameters together.

The TOE shall ensure that:

- The SCD/SVD pair is generated by the CM, allowing it to control that it is suitable for suitable for the advanced or qualified electronic signature, so that the SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD.
- The SCD/SVD pair is not usable until it is linked with the authentication factor of the signatory. It is initially disabled or already linked with those factors.
- The SCD is processed only in a form avoiding any breach of its confidentiality.
- The secrecy of the SCD (used for signature creation) is controlled by the CM, so that it can be reasonably assured against attacks with a high attack potential.
- The algorithms and algorithm parameters selected for the digital signatures are such cannot be forged without knowledge of the SCD through robust encryption techniques, and that the SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE.

Application note:

This objective corresponds to the requirements of OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy and OT.Sig_Secure for the SSCD.

> *The objective is provided by the adequate selection of the cryptographic algorithms used in the requests sent to the cryptographic module and specified by FCS_CKM.1 for the SCD/SVD generation, FCS_COP.1 for the signature operation and FCS_CKM.4 for the secure destruction of the keys.*

5.1.4 Security objectives on administration & audit

OT.USER_AUTHENTICATION Users authentication

The TOE shall authenticate Personalisation Agents, Administrators and Auditors before allowing access to assets.

The objective is provided by FIA_UID.2/USERS and FIA_UAU.2/USERS that require the personalisation agents, administrators and auditors to be authenticated before allowing any actions.

OT.ACCESS_CONTROL Access control on TOE management function

The TOE shall limit the access to assets to authenticated Personalisation Agents, Administrators and Auditors in conformity with the TSCM management access control policy.

The objective is provided by FMT_SMF.1 that defines the management functions allowed by the TSF, FMT_SMR.1/USERS that define the roles and FDP_ACC.1/MANAGEMENT and FDP_ACF.1/MANAGEMENT that require access control on the management functions. FMT_MSA.1/MANAGEMENT and FMT_MSA.3/MANAGEMENT restrict the signatory account management to personalisation agents.

OT.AUDIT Audit trail recording

The TOE shall create audit record of all significant events and allows access and analysis of such record to authorized users only.

The objective is provided by FAU_GEN.2 and FAU_GEN.1 that require the generation of audit records associated with the identity of the user that caused the event. FDP_ACC.1/MANAGEMENT and FDP_ACF.1/MANAGEMENT require access control on the audit trail.

5.2 Security Objectives for the Operational Environment

The TSP shall implement the following security objectives of the TOE operational environment.

OE.TSP Trusted Service Provider

The Trusted Service Provider that hosts the TOE shall apply applicable procedures for its operation, and operates according to the requirements laid down in [EN319401] and [EN319431] or equivalent.

OE.SECENV Protected environment

The TOE shall be operated in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE software and hardware environment shall be maintained by Administrators in a secure state.

OE.HOST_REVIEW Hosting platform review

The configuration of the hosting platform shall be regularly reviewed to detect as soon as possible the presence of uncontrolled applications.

OE.SVD_Auth Authenticity of the SVD

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others)

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- the advanced signature of the CSP.

OE.DTBS_Intend SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that:

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature result received by the TOE to the data or provides it separately.

Application note:

When the SCA used in the system in which the TOE is integrated is a CSCA that runs in the local environment of the signatory and transmits the DTBS/R to the SCC that then forwards it to the TOE, the second point is easily verified. If not then further mechanisms have to be implemented in the solution for this objective to be reached. For example, the SCC could confirm the DTBS/R value by receiving through a local channel additionally to the value received through the TOE. Otherwise when the DTBS/R consists of the DTBS, the SCC may implement means of displaying the DTBS to confirm that it’s the correct one. Instead of the full DTBS, the system may also associate initially the displayed DTBS to a shorter message which is then displayed by the SCC for confirmation. The integrity of the link between the two shall be then ensured through the cryptographic module.

Application note:

The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.DTBS_Protect SCA protects the data intended to be signed

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

OE.SAP_HSM Use of a certified SAP HSM

The HSM module shall be certified conform to [PP SAP HSM]. In particular, the HSM module shall protect the key pair against unauthorized activation or disclosure. The HSM module shall also be able to generate the TOE authentication private and public keys and to export the public key to request a certificate.

OE.SCC Use of a certified SCC

The SCC component shall be certified conform to [PP SAP] and shall be in possession of its legitimate user.

OE.SECURE CHANNEL User device – Server secure channel

The TOE environment shall provide mechanisms to answer to creation request of a secure channel between the user device and the server hosting the TOE and to manage exchange in the secure channel to assure confidentiality and integrity of data exchange in the secure channel.

OE.CRYPTO Use of cryptography

The SAP HSM module shall be configured to use cryptographic functions which level of security is in accordance with the rules and recommendations defined by the TSP policy.

OE.SIGNATORY Security obligation of the signatory

The signatory shall keep their VAD confidential.

OE.AUDIT_REVIEW Review of the audit trail

The Auditors shall check the audit trails on a regular basis, and shall notify the corresponding authority in the case that an incident occurred

5.3 Security Objective Rationale

The following table provides an overview for security objectives coverage in the base-PP.

	A.TSP	A.SECENV	A.CGA	A.SCA	A.SCC	A.SAP_HSM	A.AUDIT_REVIEW	T.ILLICIT_REQUEST	T.UNAUTHORIZED_PERSONNALISATION	T.SCC_IMPERSONATION_ENR	T.SCC_IMPERSONATION	T.SCC_TSCM_MANINTHEMIDDLE	T.UNAUTHORIZED_SIG	T.DTBS_Forgery	T.SCD_Derive	T.SVD_Forgery	T.Sig_Forgery	T.PRIVILEGE_ESCALATION	T.AUDIT_ALTERATION	OSP.Personalisation	OSP.TSP_Sigy_Policy	OSP.CSP_QCert	OSP.QSign	OSP.Sigy_RSCD	OSP.Sig_Non-Repud
OT.SCC_KEY_ENR										X										X					
OT.SCD/SVD_Auth_Gen															X										
OT.QCert_Request																						X			
OT.TSCM_AUTHENTICATION												X													
OT.SCC_AUTHENTICATION											X	X													
OT.REQUEST_AUTHENTICATION								X																	
OT.SIGNATURE_ACTIVATION_PROTECTION													X										X	X	X
OT.DTBS_Integrity_TOE													X	X											
OT.CM_SECURE_CRYPTO															X	X	X						X	X	X
OT.USER_AUTHENTICATION									X									X	X	X	X	X			
OT.ACCESS_CONTROL									X									X	X	X	X	X			
OT.AUDIT									X									X			X				
OE.TSP	X																								
OE.SECENV		X																							
OE.HOST_REVIEW																		X							
OE.SVD_Auth			X													X									X
OE.CGA_QCert			X														X					X	X		X
OE.DTBS_Intend				X									X	X											
OE.DTBS_Protect													X	X											
OE.SAP_HSM						X									X									X	X
OE.SCC					X					X	X														
OE.SECURE CHANNEL												X													

	A.TSP	A.SECENV	A.CGA	A.SCA	A.SCC	A.SAP_HSM	A.AUDIT_REVIEW	T.ILLICIT_REQUEST	T.UNAUTHORIZED_PERSONNALISATION	T.SCC_IMPERSONATION_ENR	T.SCC_IMPERSONATION	T.SCC_TSCM_MANINTHEMIDDLE	T.UNAUTHORIZED_SIG	T.DTBS_Forgery	T.SCD_Derive	T.SVD_Forgery	T.Sig_Forgery	T.PRIVILEGE_ESCALATION	T.AUDIT_ALTERATION	OSP.Personalisation	OSP.TSP_Sigy_Policy	OSP.CSP_QCert	OSP.QSign	OSP.Sigy_RSCD	OSP.Sig_Non-Repud
OE.CRYPTO															X									X	X
OE.SIGNATORY													X												
OE.AUDIT_REVIEW							X		X									X							

6 Security Requirements

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

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in *italicized* text and the added/changed words are in *italicized* text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets 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 that have been made by the PP authors are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized like *this*.

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.

6.1 Security Functional Requirements

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

6.1.1 Subjects, Operations and Objects

The following table contains the list of subjects that interact with the TOE and describes the security attributes of each subject.

Subject	Description	Security attributes	Possible values	Default value
S.Signatory	The subject S.Sigy is acting in the role R.Sigy after a successful authentication of the user as signatory.	Authentication status as Signatory	Authenticated Not authenticated	Not authenticated
S.Administrator	The subject S.Admin is acting in the role R.Admin after a successful authentication of the user as administrator.	Authentication status as Administrator	Authenticated Not authenticated	Not authenticated
S.EnrolAgent	The subject S.EnrolAgent is acting in the role R.EnrolAgent after a successful authentication of the user as Personalisation Agent.	Authentication status as EnrolAgent	Authenticated Not authenticated	Not authenticated

Subject	Description	Security attributes	Possible values	Default value
S.Auditor	The subject S.Auditor is acting in the role R.Auditor after a successful authentication of the user as auditor.	Authentication status as Auditor	Authenticated Not authenticated	Not authenticated
S.SCA	The subject S.SCA is acting in the role R.SCA after a successful authentication as a Signature Creation Application.	Authentication status as SCA	Authenticated Not authenticated	Not authenticated
S.SCC	The subject S.SCC is acting in the role R.SCC after a successful authentication as a Sole Control Component.	Authentication status as SCC	Authenticated Not authenticated	Not authenticated

Table 2: List of subjectThe following table contain the list of objects handled by the TOE and describes their security attributes.

Object	Description	Security attributes	Possible values	Default value
Signature request	Request received from the SCA for a specified signatory and one of his SCD, and for a specified DTBS/R	Status	Received (In Progress) Authenticated Verified (only after SAD successful verification) Done	Received
DTBS/R	Representation of the data to be signed, received from the SCA	Integrity seals	Not Yet Received Valid Invalid	Not Yet Received
Signatory account	Account of each signatory declared to the TSCM	Signatory account status	Blocked Unblocked (after signatory authentication)	Blocked
Certificate request	Request for certificate generation sent to the CGA	Certificate subject	Defined by the CGA policy	Signatory identity
User account	Account of each TSCM users: administrators, personalisation agents and auditors	User account status	Blocked Unblocked (after user authentication)	Blocked
Audit trail	Logs of the operations done by the TOE			

Table 3: List of objects

The following table contain the list of operations that the subjects can perform on the identified objects.

Subject	Operations	Objects	Phase

Subject	Operations	Objects	Phase
S.Signatory with his SCA	Request signature creation	Signature request	Operational phase
S.EnrolAgent	Creation, initialization and update of signatory accounts, including: SCC enrolment (if available) request of SCD/SVD generation in the cryptographic module certificate request to the CGA certificate installation	Signatory account	Signatory account creation and initialization
S.Administrator	Creation, initialization and update of users' accounts	Users' accounts	Operational phase
S.Auditor	Audit trail review	Audit trail	Operational phase

Table 4: List of operations

6.1.2 Extended Requirements

This protection profile uses components defined as extensions to CC part 2.

6.1.2.1 Extended Family FIA_API - Authentication Proof of Identity

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.

6.1.2.2 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.

6.1.3 Security Functional Requirements on enrolment

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

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

Satisfied dependencies: FDP_ACC.1/ENR, FPT_TDC.1/ENR

Rationale for non satisfied dependencies: the FTP_ITC.1 component is not required because the trusted channel between the TOE and the SCC can be provided by the TOE environment (cf. OE.SECURE_CHANNEL)

FDP_ITC.2.1 The TSF shall enforce the Enrolment access control policy when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

Refinement: user data here are the SCC_ID and the SCC_RAD of the SCC owned by the signatory

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

Required dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret the SCC_ID and the SCC_RAD of the SCC owned by the signatory when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 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.

Refinement: the trusted IT product here is the SCC.

FDP_ACC.1/ENR Subset access control

Required dependencies: FDP_ACF.1 Security attribute based access control

Satisfied dependencies: FDP_ACF.1/ENR

FDP_ACC.1.1 The TSF shall enforce the Enrolment access control policy on Signatory account creation and initialization.

FDP_ACF.1/ENR Security attribute based access control

Required dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation

Satisfied dependencies: FDP_ACC.1/ENR, FMT_MSA.3/ENR

FDP_ACF.1.1 The TSF shall enforce the Enrolment access control policy to objects based on the following: S.EnrolAgent (authentication status) subject, Signatory account creation, initialization and update operation.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: only authenticated personalisation agents (S.EnrolAgent) are allowed to perform Signatory account creation, initialization and update.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: Signatory account creation and initialization is not allowed without personalisation agent (S.EnrolAgent) authentication.

FMT_MSA.3/ENR Static attribute initialisation

Required dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

Satisfied dependencies: FMT_MSA.1/ENR, FMT_SMR.1/USERS

FMT_MSA.3.1 The TSF shall enforce the Enrolment access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the personalisation agent (S.EnrolAgent) to specify alternative initial values to override the default values when an object or information is created.

Refinement: default values here are default values for security attributes of the signatories' accounts.

FMT_MSA.1/ENR Management of security attributes

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

Satisfied dependencies: FDP_ACC.1/ENR, FMT_SMR.1/USERS, FMT_SMF.1

FMT_MSA.1.1 The TSF shall enforce the Enrolment access control policy to restrict the ability to change_default, query, modify, delete the security attributes Signatory account attributes as defined in Table 3 to personalisation agents (S.EnrolAgent).

FCS_CKM.1 Cryptographic key generation

Required dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction

Satisfied dependencies: FCS_COP.1, FCS_CKM.4

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

Refinement: cryptographic keys here are the SCD/SVD key pair for a signatory.

Application Note:

The TOE shall request the generation of the keys to the HSM and shall import the SCD_ID and the SVD after the successful generation. The SVD is used to request the certificate to the CGA.

FCS_CKM.4 Cryptographic key destruction

Required dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

Satisfied dependencies: FCS_CKM.1

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

Refinement: cryptographic keys here are SCD/SVD pair.

Application Note:

When needed, the TOE shall request the destruction of the keys to the HSM.

FCO_NRO.2/CSR Enforced proof of origin

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: the identity of the signatory is provided by FDP_ITC.2/RAUTH in case of HOLDER-SIDE AUTHENTICATION or FIA_UID.2/SIGNATORY in case of SERVER-SIDE AUTHENTICATION.

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted certificate requests at all times.

FCO_NRO.2.2 The TSF shall be able to relate the identity of the originator of the information, and the certificate subject field of the information to which the evidence applies.

Refinement: the identity of the originator is here the identity of the signatory requesting a certificate for his public signature key.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to the recipient given the signature of the certificate request.

Refinement: the recipient id here the CGA. The origin of the certificate request is assured by the signature of the certificate request by the private key only owned by the signatory. This signature assures that the origin of the request is the signatory.

6.1.4 Security Functional Requirements on TSCM authentication

FIA_API.1 Authentication Proof of Identity

Required dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the TOE to an external entity.

6.1.5 Security Functional Requirements on SCC authentication

FIA_UID.2/SCC User identification before any action

Required dependencies: No dependencies.

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

Refinement: users here are SCC devices.

FIA_UAU.2/SCC User authentication before any action

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: FIA_UID.2/SCC

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

Refinement: users here are SCC devices.

6.1.6 Security Functional Requirements on signature operations

FIA_UID.2/REQUEST User identification before any action

Required dependencies: No dependencies.

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

Refinement: users here are the origin of the signature request (SCA or SCC on behalf of signatory)

FIA_UAU.2/REQUEST User authentication before any action

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: FIA_UID.2/REQUEST

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

Refinement: users here are the origin of the signature request (SCA or SCC)

FCS_COP.1 Cryptographic operation

Required dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction

Satisfied dependencies: FCS_CKM.1, FCS_CKM.4

FCS_COP.1.1 The TSF shall perform signature creation 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*].

FDP_ACC.1/SIGNATURE Subset access control

Required dependencies: FDP_ACF.1 Security attribute based access control

Satisfied dependencies: FDP_ACF.1/SIGNATURE

FDP_ACC.1.1 The TSF shall enforce the Signature access control policy on Signature requests.

FDP_ACF.1/SIGNATURE Security attribute based access control

Required dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation

Satisfied dependencies: FDP_ACC.1/SIGNATURE

Rationale for non-satisfied dependencies: FMT_MSA.3 component is not required because the status of the signature request is not manageable by one of the TSCM users (personalisation agents, administrators, auditors)

FDP_ACF.1.1 The TSF shall enforce the Signature access control policy to objects based on the following: Signature request (status).

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: signature creation for a specified signatory and one of his SCD, and for a specified DTBS/R is allowed only if the status of the request is Verified meaning that the SAD generated by the signatory with his SCC has been successfully verified.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: signature creation is not allowed without SAD successful verification.

FDP_SDI.2/DTBSR Stored data integrity monitoring and action

Required dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: DTBS/R integrity seals.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall:

1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error

6.1.7 Security Functional Requirements on administration and audit

FMT_SMF.1 Specification of Management Functions

Required dependencies: No dependencies.

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

- Signatory account creation, initialization and update
- User account (Admin, PA, Auditor) creation, initialization and update
- Role management
- Audit trail review

FMT_SMR.1/USERS Security roles

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: FIA_UID.2/USERS

FMT_SMR.1.1 The TSF shall maintain the roles personalisation agent (S.EnrolAgent), administrator (S.Administrator) and auditor (S.Auditor).

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

FIA_UID.2/USERS User identification before any action

Required dependencies: No dependencies.

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

Refinement: users here are personalisation agent (S.EnrolAgent), administrator (S.Administrator) and auditor (S.Auditor).

FIA_UAU.2/USERS User authentication before any action

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: FIA_UID.2/USERS

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

Refinement: users here are personalisation agent (S.EnrolAgent), administrator (S.Administrator) and auditor (S.Auditor).

FDP_ACC.1/MANAGEMENT Subset access control

Required dependencies: FDP_ACF.1 Security attribute based access control

Satisfied dependencies: FDP_ACF.1/MANAGEMENT

FDP_ACC.1.1 The TSF shall enforce the TSCM management access control policy on TSCM management operations (TSCM authentication key generation and export, Role management, Audit trail review).

FDP_ACF.1/MANAGEMENT Security attribute based access control

Required dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation

Satisfied dependencies: FDP_ACC.1/MANAGEMENT, FMT_MSA.3/MANAGEMENT

FDP_ACF.1.1 The TSF shall enforce the TSCM management access control policy to objects based on the following: S.Administrator (authentication status) and S.Auditor (authentication status) subjects, TSCM management operations (users' account creation, initialization and update, Audit trail review).

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

- only authenticated administrators (S.Administrator) are allowed to create, initialize and to update user accounts,
- only authenticated auditors (S.Auditor) are allowed to perform audit trail review.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: TSCM management operations (users accounts creation, initialization and update, Audit trail review) are not allowed without administrator (S.Administrator) or auditor (S.Auditor) authentication.

FMT_MSA.3/MANAGEMENT Static attribute initialisation

Required dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

Satisfied dependencies: FMT_MSA.1/MANAGEMENT, FMT_SMR.1/USERS

FMT_MSA.3.1 The TSF shall enforce the TSCM management access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the administrator (S.Administrator) to specify alternative initial values to override the default values when an object or information is created.

Refinement: default values here are default values for security attributes of the users' accounts.

FMT_MSA.1/MANAGEMENT Management of security attributes

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

Satisfied dependencies: FDP_ACC.1/ENR, FMT_SMR.1/USERS, FMT_SMF.1

FMT_MSA.1.1 The TSF shall enforce the TSCM management access control policy to restrict the ability to change_default, query, modify, delete the security attributes Users' accounts attributes as defined in Table 3 to administrators (S.Administrator).

FAU_GEN.1 Audit data generation

Required dependencies: FPT_STM.1 Reliable time stamps

Satisfied dependencies: FPT_STM.1 is not required because the TOE relies on the system time to timestamp audit events and it is assumed (A.SECENV) that this time is reliable.

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the minimum level of audit; and

c) [assignment: *other specifically defined auditable events*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

SFR	Auditable events
FDP_ITC.2/ENR	Successful import of user data (SCC information), including any security attributes
FPT_TDC.1/ENR	Successful use of TSF data (SCC information) consistency mechanisms
FDP_ACC.1/ENR	-
FDP_ACF.1/ENR	-
FMT_MSA.3/ENR	-
FMT_MSA.1/ENR	Success and failure in management of security attributes
FCS_CKM.1	Success and failure of the activity (signatory keys generation)
FCS_CKM.4	Success and failure of the activity (signatory keys destruction)
FCO_NRO.2/CSR	The invocation of the non-repudiation service
FIA_UID.2/SCC	Unsuccessful use of the user (SCC) identification mechanism, including the user identity provided

SFR	Auditable events
FIA_UAU.2/SCC	Unsuccessful use of the authentication mechanism
FIA_UID.2/REQUEST	Unsuccessful use of the user (signature request) identification mechanism, including the user identity provided
FIA_UAU.2/REQUEST	Unsuccessful use of the authentication mechanism
FCS_COP.1	Success and failure, and the type of cryptographic operation (signature)
FDP_ACC.1/SIGNATURE	-
FDP_ACF.1/SIGNATURE	-
FDP_SDI.2/DTBSR	Successful attempts to check the integrity of user data (DTBS/R), including an indication of the results of the check
FMT_SMF.1	Use of the management functions
FMT_SMR.1/USERS	Modifications to the group of users that are part of a role
FIA_UID.2/USERS	Unsuccessful use of the user (administrators, personalization agents, auditors) identification mechanism, including the user identity provided
FIA_UAU.2/USERS	Unsuccessful use of the authentication mechanism
FDP_ACC.1/MANAGEMENT	-
FDP_ACF.1/MANAGEMENT	-
FMT_MSA.3/MANAGEMENT	-
FMT_MSA.1/MANAGEMENT	-
FAU_GEN.1	-
FAU_GEN.2	-

Table 5: List of auditable events (base-PP)

FAU_GEN.2 User identity association

Required dependencies: FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification

Satisfied dependencies: FAU_GEN.1, FIA_UID.2/USERS and FIA_UID.2/SCC

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

6.2 Security Assurance Requirements for the TOE

The required security assurance level is **Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2 and AVA_VAN.5** components.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

	OT.SCC_KEY_ENR	OT.QCert_Request	OT.SCC_AUTHENTICATION	OT.REQUEST_AUTHENTICAITON	OT.SIGNATURE_ACTIVATION_PROTECTION	OT.DTBS_Integrity_TOE	OT.SCD/SVD_Auth_Gen	OT.CM_SECURE_CRYPTO	OT.USER_AUTHENTICATION	OT.ACCESS_CONTROL	OT.AUDIT
FDP_ITC.2/ENR	X										
FPT_TDC.1/ENR	X										
FDP_ACC.1/ENR	X	X					X				
FDP_ACF.1/ENR	X	X					X				
FMT_MSA.3/ENR	X										
FMT_MSA.1/ENR	X										
FCS_CKM.1								X			
FCS_CKM.4								X			
FCO_NRO.2/CSR		X									
FIA_UID.2/SCC			X								
FIA_UAU.2/SCC			X								
FIA_UID.2/REQUEST				X							
FIA_UAU.2/REQUEST				X							
FCS_COP.1								X			
FDP_ACC.1/SIGNATURE					X						
FDP_ACF.1/SIGNATURE					X						
FDP_SDI.2/DTBSR						X					
FMT_SMF.1										X	
FMT_SMR.1/USERS										X	
FIA_UID.2/USERS									X		
FIA_UAU.2/USERS									X		
FDP_ACC.1/MANAGEMENT										X	X
FDP_ACF.1/MANAGEMENT										X	X
FMT_MSA.3/MANAGEMENT										X	
FMT_MSA.1/MANAGEMENT										X	
FAU_GEN.1											X
FAU_GEN.2											X

Table 6 - Coverage of Security Objective for the TOE by SFR

6.3.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The satisfaction of the required dependencies is available in the description of each security functional requirement is section 6.1.

6.3.3 Security Assurance Requirements Rationale

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.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the development and manufacturing process.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

The component AVA_VAN.5 augmented to EAL4 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these are met or exceeded in the EAL4 assurance package.

7 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
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
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 Provider	Trust Service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of digital 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

Acronym	Term
CC	Common Criteria
AdES	Digital signature in CADES, XADES or PADES format
CM	Cryptographic Module
CGA	Certificate Generation Application
DTBS	Data To Be Signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation assurance level
EC	European Commission
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalisation Terminal
RAD	Reference authentication data
RSCD	Remote Signature Creation Device
SAP	Signature Activation Protocol
SAD	Signature Activation Data
SAR	Security assurance requirements
SFR	Security functional requirement
SCA	Signature Creation Application
SCC	Sole Control Component
SCD	Signature Creation Data
SDO	Signed data object
SCDev	Signature Creation Device
SD	Signers’ Document
QSCD	Qualified Signature Creation Device
TW4S	Trustworthy System Supporting Server Signing
TOE	Target of Evaluation
TSF	TOE security functions
VAD	Verification Authentication Data

8 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[5] CC and CEM addenda, modular PP; CCMB-2014-03-001, Version 1.0, March 2014

Cryptography

[6] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[7] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[8] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[9] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[10] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[11] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

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

[13] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

Protection Profiles

[14] [PP SAP HSM] Protection Profile for Signature Activation Protocol (SAP) management SAP HSM module

[15] [PP SAP] Protection profile on Signature Activation Protocol (SAP) management

[16] [PP TSCM] This document : Protection profile for Trustworthy Signature Creation Module in TW4S

[17] [PP SCA] EN 419 211-2 Protection profiles for signature creation and verification application - Signature creation application – Part 2: Core PP

[18] [PP SSCD] EN 419 221-2 Protection profiles for secure signature creation device — Part 2: Device with key generation

ETSI and CEN standard

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

[20] [ISO-27115] ISO/IEC JTC 1/SC 27 Information technology — Security techniques — Entity authentication assurance framework – December 2012 - ISO/IEC FDIS 29115: 2012

[21] [ISO-24760] ISO/IEC 24760-1:2011, Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.

[22] [ISO-7816-4] ISO/IEC 7816-4:2013, Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange.

[23] [ISO-29115] ISO/IEC 29115:2013, Information Technology – Security Techniques – Entity Authentication Assurance Framework.

Other

[24] 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

Appendix A HOLDER-SIDE AUTHENTICATION modular-PP

This appendix specifies the elements to be included in a security target claiming conformance with the HOLDER-SIDE AUTHENTICATION configuration.

Security Problem Definition

Assets

There is not any specific asset in this module. All assets are described in 4.1.

Threats

There is not any specific threat in this module. The main objective of this module-PP is to refine the coverage of T.UNAUTHORIZED_SIGNATURE_ACTIVATION when the signatory is authenticated by the SCC.

In this case, the rationale of coverage of the threat is:

> *T.UNAUTHORIZED_SIGNATURE_ACTIVATION is countered by OT.GET_SIGNATORY_AUTHENTICATION that requires the authentication of the signatory. OT.SIGNATURE_ACTIVATION_PROTECTION ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.SIGNATORY ensures also that the signatory keeps their VAD confidential.*

Security Objectives for the TOE

OT.GET_SIGNATORY_AUTHENTICATION

The TOE shall check that the signatory has been authenticated by the SCC and shall get the signatory identification from the SCC.

> *The objective is provided by FDP_ITC.2/RAUTH that requires the importation of the holder-side authentication confirmation and FPT_TDC.1/RAUTH that requires the TOE to be able to interpret the data received from the SCC. FDP_IFC.1/RAUTH and FDP_IFF.1/RAUTH require to authenticate the source that sent the signatory authentication confirmation before to consider the signatory being authenticated.*

Security Requirements

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

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

Satisfied dependencies: FDP_IFC.1/RAUTH, FPT_TDC.1/AUTH

Rationale for non satisfied dependencies: the FTP_ITC.1 component is not required because the trusted channel between the TOE and the SCC can be provided by the TOE environment (cf. OE.SECURE_CHANNEL)

FDP_ITC.2.1 The TSF shall enforce the holder-side authentication confirmation policy when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

Refinement: user data are here the confirmation of authentication sent by the SCC.

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

Required dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret the confirmation of authentication sent by the SCC when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 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.

Refinement: the trusted IT product here is the SCC.

FDP_IFC.1/RAUTH Subset information flow control

Required dependencies: FDP_IFF.1 Simple security attributes

Satisfied dependencies: FDP_IFF.1/RAUTH

FDP_IFC.1.1 The TSF shall enforce the holder-side authentication confirmation policy on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

FDP_IFF.1/RAUTH Simple security attributes

Required dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation

Satisfied dependencies: FDP_IFC.1/RAUTH, FMT_MSA.3/ENR for the enrolment of the SCC

FDP_IFF.1.1 The TSF shall enforce the holder-side authentication confirmation policy based on the following types of subject and information security attributes: signatory authentication confirmation with the associated source SCC as security attributes.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: the signatory is considered as authenticated only if the source SCC of the signatory authentication has been successfully authenticated.

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: the source SCC that performed the signatory authentication is authenticated.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: the source that declares having performed the signatory authentication is not authenticated.

SFR	Auditable events

SFR	Auditable events
FDP_ITC.2/RAUTH	Successful import of user data (confirmation of authentication), including any security attributes
FPT_TDC.1/RAUTH	Successful use of TSF data (confirmation of authentication) consistency mechanisms
FDP_IFC.1/RAUTH	-
FDP_IFF.1/RAUTH	-

Table 7: List of auditable events (HOLDER-SIDE AUTHENTICATION module-PP)

Appendix B SERVER-SIDE AUTHENTICATION modular-PP

This appendix specifies the elements to be included in a security target claiming conformance with the SERVER-SIDE AUTHENTICATION configuration.

Security Problem Definition

Asset

In the SERVER-SIDE AUTHENTICATION configuration, the TOE needs to handle additional assets.

D.SIGNATORY_RAD

This asset is the signatory reference authentication data used to perform comparison with the signatory verification authentication data in order to allow signatory authentication.

Protection: integrity and confidentiality.

D.SIGNATORY_VAD_REMOTE

This asset is the signatory verification authentication transient data transferred to TOE for signatory authentication.

Protection: integrity and confidentiality

Threats

The main objective of this module-PP is to refine the coverage of T.UNAUTHORIZED_SIGNATURE_ACTIVATION when the signatory is authenticated by the TOE. The rationale

In this case, the rationale of coverage of the threat is:

> *T.UNAUTHORIZED_SIGNATURE_ACTIVATION is countered by OT.TSCM_SIGNATORY_AUTHENTICATION that requires the authentication of the signatory. OT.SIGNATURE_ACTIVATION_PROTECTION ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.SIGNATORY ensures also that the signatory keeps their VAD confidential.*

But additional threats are also introduced by this configuration.

T.SIGNATORY_IMPERSONATION_ENR

An attacker impersonates a legitimate signatory during the enrolment phase:

- by bypassing identity information verification,
- by presenting counterfeited identity documents during identity information verification,
- by obtaining the creation of an illegitimate account from the personalisation agent,
- by gaining access to the signatory RAD during its generation, its storage or its transfer to the signatory,
- by altering or replacing holder 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 the TOE

> *T.SIGNATORY_IMPERSONATION_ENR is mainly countered by OT.SIGNATORY_RAD_ENR and OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL requiring personalisation agents to be authenticated to perform personalisation operations. OE.RAD_STORAGE requires the storage of the RAD in the HSM.*

T.SIGNATORY_IMPERSONATION_REMOTE

An attacker impersonates a signatory in operational phase using several means as:

- forgering signatory authentication data,
- obtaining holder credential unsecurely stored by issuer or holder,
- disclosure of VAD during transfer between SCC and TOE ([ISO-29115] T.Eavesdropping),
- disclosure during comparison of VAD with RAD in TOE,
- 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 the TOE

> *T.SIGNATORY_IMPERSONATION_REMOTE is countered by OT.TSCM_SIGNATORY_AUTHENTICATION requiring an authentication mechanism resistant to attacker with a high attack potential.*

T.SIGN_CREDENTIAL_UNAUTHORIZED_UPDATE Unauthorized update of Signatory credentials

An attacker impersonates a signatory to perform an unauthorized update of his credentials.

> *T.SIGN_CREDENTIAL_UNAUTHORIZED_UPDATE is countered by OT.SIGNATORY_RAD_UPDATE requiring a secure update mechanism.*

T.SIGN_CREDENTIAL_DISCLOSURE Disclosure of Signatory credentials during update

An attacker discloses signatory credentials (RAD) during the update operation.

> *T.SIGN_CREDENTIAL_DISCLOSURE is countered by OT.SIGNATORY_RAD_UPDATE requiring a secure update mechanism.*

Security Objectives for the TOE

OT.TSCM_SIGNATORY_AUTHENTICATION

The TOE shall securely authenticate the signatory, using the RAD stored in the SAP HSM. Confidentiality of the signatory VAD is required during its transfer between the SCC and the TOE.

> *The objective is provided by FIA_UID.2/SIGNATORY and FIA_UAU.2/SIGNATORY that require signatory authentication.*

OT.SIGNATORY_RAD_ENR

The TOE shall be able to import the Signatory RAD in the TOE during personalisation phase.

> *The objective is provided by FDP_ITC.2/SIGNATORY for the import of the signatory RAD and FPT_TDC.1/SIGNATORY that requires the TOE to be able to interpret the signatory RAD during the enrolment.*

OT.SIGNATORY_RAD_UPDATE

The TOE may be able to securely update the Signatory RAD during operational phase.

The objective is provided by FDP_ITC.2/SIGNATORY for the import of the signatory RAD and FPT_TDC.1/SIGNATORY that requires the TOE to be able to interpret the signatory RAD during the update.

OE.RAD_STORAGE

The SAP HSM shall ensure the protection of the RAD stored in the HSM.

Security Requirements

FIA_UID.2/SIGNATORY User identification before any action

Required dependencies: No dependencies.

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

Refinement: users here are signatories.

FIA_UAU.2/SIGNATORY User authentication before any action

Required dependencies: FIA_UID.1 Timing of identification

Satisfied dependencies: FIA_UID.2/SIGNATORY

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

Refinement: users here are signatories.

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

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

Satisfied dependencies: FDP_ACC.1/ENR, FPT_TDC.1/SIGNATORY

Rationale for non satisfied dependencies: the FTP_ITC.1 component is not required because the trusted channel between the TOE and the SCC can be provided by the TOE environment (cf. OE.SECURE_CHANNEL)

FDP_ITC.2.1 The TSF shall enforce the Enrolment access control policy when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

Refinement: user data here are the signatory RAD

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

Required dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret the signatory RAD when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 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.

Refinement: the trusted IT product here is the device used by the signatory to enrol or to update his RAD.

SFR	**Auditable events**
FIA_UID.2/SIGNATORY	Unsuccessful use of the user identification mechanism, including the user identity provided
FIA_UAU.2/SIGNATORY	Unsuccessful use of the authentication mechanism
FDP_ITC.2/SIGNATORY	Successful import of user data (signatory RAD), including any security attributes
FPT_TDC.1/SIGNATORY	Successful use of TSF data (signatory RAD) consistency mechanisms

Table 8: List of auditable events (SERVER-SIDE AUTHENTICATION module-PP)

Appendix C PRIVACY modular-PP

This appendix specifies the elements to be included in a security target claiming conformance with the PRIVACY configuration.

Security Problem Definition

Assets

In the PRIVACY configuration, the TOE needs to handle additional protection requirements for the assets.

D.DTBSR_C

This asset is the addition to D.DTBSR when confidentiality is required to assure signatory privacy.

Protection: Confidentiality

D.SIGN_REQUEST_C

This asset is the addition to D.SIGN_REQUEST when confidentiality is required to assure signatory privacy.

Protection: Confidentiality

D.IDENTIFICATION_DATA_C

This asset is the addition to D.IDENTIFICATION_DATA when confidentiality is required to assure signatory privacy.

Protection: Confidentiality

Threats

T.SCA_COMM_EAVESDROP

An attacker having access to the communication channel between the SCA and the TSCM passively eavesdrops the exchanged data to obtain information that could be used to obtain sensitive data about the signature (D.DTBSR_C, D.SIGN_REQUEST_C, and D.IDENTIFICATION_DATA_C).

> *T.SCA_COMM_EAVESDROP is countered by OT.SCA-TSCM_SECURE_CHANNEL that requires the creation of a secure channel between the SCA and the TOE.*

T.SCC_COMM_EAVESDROP

An attacker having access to the communication channel between the SCC and the TSCM passively eavesdrops the exchanged data to obtain information that could be used to obtain sensitive data about the signature (D.DTBSR_C, D.SIGN_REQUEST_C, and D.IDENTIFICATION_DATA_C).

> *T.SCC_COMM_EAVESDROP is countered by OT.SCC-TSCM_SECURE_CHANNEL that requires the creation of a secure channel between the SCC and the TOE.*

T.UNAUTHORISED_ACCESS

An attacker having access to the server hosting the TOE gains access to the sensitive data about the signature (D.DTBSR_C, D.SIGN_REQUEST_C, and D.IDENTIFICATION_DATA_C).

> *T.UNAUTHORISED_ACCESS is countered by OT.USER_AUTHENTICATION and OT.ACCESS_CONTROL restricting the access to sensitive data to authenticated administrators and OE.SECENV restricting the access to the server.*

Security Objectives for the TOE

OT.SCA-TSCM_SECURE_CHANNEL

The TOE shall be able to establish a secure channel between the SCA and the TOE to protect the confidentiality of the DTBS/R, of the signature request content and of the signatory identification data during their transfer.

> *The objective is provided by FTP_ITC.1/SCA_PRIVACY that requires the creation of a trusted channel between the TOE and the SCC locally distinct from the secure channel supported by the server and the user device.*

OT.SCC-TSCM_SECURE_CHANNEL

The TOE shall be able to establish a secure channel between the SCC and the TOE to protect the confidentiality of the DTBS/R, of the signature request content and of the signatory identification data during their transfer.

> *The objective is provided by FTP_ITC.1/SCC_PRIVACY that requires the creation of a trusted channel between the TOE and the SCC locally distinct from the secure channel supported by the server and the user device.*

Security Requirements

FTP_ITC.1/SCA_PRIVACY Inter-TSF trusted channel

Required dependencies: No dependencies.

FTP_ITC.1.1 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 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for the transfer of DTBS/R, signature requests and signatory identification data between the SCA and the TOE.

FTP_ITC.1/SCC_PRIVACY Inter-TSF trusted channel

Required dependencies: No dependencies.

FTP_ITC.1.1 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 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for the transfer of DTBS/R, signature requests and signatory identification data between the TOE and the SCC.

SFR	Auditable events
FTP_ITC.1/SCA_PRIVACY	Failure of the trusted channel functions
FTP_ITC.1/SCC_PRIVACY	Failure of the trusted channel functions

Table 9: List of auditable events (PRIVACY module-PP)

Appendix D EXTERNAL KEY STORAGE modular-PP

This appendix specifies the elements to be included in a security target claiming conformance with the EXTERNAL KEY STORAGE configuration.

When the HSM provides features to securely store the signatories’ keys out of the cryptographic module, the TOE needs to manage the SCD exportation and importation when necessary. This function is not required if the SAP HSM is able to store all signatories’ keys and never requires them to be exported.

Security Problem Definition

Assets

In the EXTERNAL KEY STORAGE configuration, the TOE needs to handle additional assets.

D.SCD_BACKUP

This asset is the backup of the SCD. The detailed content of this asset is not known by the TOE that only needs to manage a full backup of both the SCD and all its associated security attributes which can be restore when needed.

Protection: integrity and confidentiality.

Threats

T.SCD_Backup_Forgery

An attacker analyse the backup of a SCD to gain access to the SCD or to alter the content of the backup (for example to associate it with another user).

> *T.SCD_Backup_Forgery is countered by OT.MANAGE_KEY_BACKUP ensuring that the link between the backup and the signatory is preserved so that the key is instantiated when needed. OE.SAP_HSM_BACKUP protects the backup with the adequate security mechanism so that an attacker cannot obtain knowledge of the SCD from the backup, and cannot modify its security attributes or restore it in the SAP HSM with different security attributes in order to destroy or to alter the association with the signatory.*

Security Objectives for the TOE

OT.MANAGE_KEY_BACKUP

The TOE shall provide security features to store the backup of the SCD created by the SAP HSM with a link to the Signatory ID, and to be able to restore it in the SAP HSM when needed (i.e. when a signature request is received for the Signatory).

> *The objective is provided by FDP_ETC.2/EXT for the secure export of the SCDs out of the HSM and FDP_ITC.2/EXT and the restoration when needed. FDP_IFC.1/EXT and FDP_IFF.1/EXT define the rules to be applied during the restoration.*

Security Objectives for the environment

OE.SAP_HSM_BACKUP

The SAP HSM shall provide security feature to backup securely the SCDs and their security attributes (protection in integrity and in confidentiality), and to restore it when needed.

Security Requirements

The following table contain the list of objects handled by the TOE and describes their security attributes.

Object	Description	Security attributes	Possible values	Default value
Signatory SCDs external storage	External copy of the signatory SCD	Seals permitting to check integrity of the data	-	Value computed at the export of the data out of the HSM

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

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

Satisfied dependencies: FDP_IFC.1/EXT

FDP_ETC.2.1 The TSF shall enforce the external storage policy when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*].

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

Required dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

Satisfied dependencies: FDP_IFC.1/EXT

Rationale for not satisfied dependencies: FTP_ITC.1 and FPT_TDC.1 are not required because it the HSM that shall provide such protection functions

FDP_ITC.2.1 The TSF shall enforce the external storage policy when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

FDP_IFC.1/EXT Subset information flow control

Required dependencies: FDP_IFF.1 Simple security attributes

Satisfied dependencies: FDP_IFF.1/EXT

FDP_IFC.1.1 The TSF shall enforce the external storage policy on signatories' SCDs external storage.

FDP_IFF.1/EXT Simple security attributes

Required dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation

Satisfied dependencies: FDP_IFC.1/EXT, FMT_MSA.3/ENR for the enrolment of the SCC

FDP_IFF.1.1 The TSF shall enforce the external storage policy based on the following types of subject and information security attributes: signatories' SCDs external storage and their attributes permitting to check their integrity.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: the restoration of the signatories' SCDs is allowed only if their integrity has been successfully checked.

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: the SCDs can be restored if their integrity is successfully checked.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: the SCDs are not restored if their integrity cannot be successfully checked.

SFR	Auditable events
FDP_ETC.2/EXT	Successful export of information (keys external copy)
FDP_ITC.2/EXT	Successful import of user data (key external copy), including any security attributes
FDP_IFC.1/EXT	-
FDP_IFF.1/EXT	-

Table 10: List of auditable events (EXTERNAL KEY STORAGE module-PP)