prEN 14169-3:2012 (E)

CEN/TC 224

Date: 2012-07

prEN 14169-3:2012

CEN/TC 224

Secretariat: AFNOR

Protection profiles for secure signature creation device — Part 3: Device with key import

Schutzprofile sichere Signaturerstellungseinheit — Teil 3: Gerät mit Schlüsselimport

Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 3: Dispositif avec import de clé

ICS:

Descriptors:

Contents

Foreword

This document (prEN 14169-3:2012) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

This document is a working document.

Introduction

This series of European standards specifies Common Criteria protection profiles for secure signature creation devices and is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2002, Annex B and Annex C on the protection profile secure signature creation devices, "EAL 4+".

This series of European standards consists of the following parts:

- Protection profiles for secure signature creation device — Part 1: Overview;
- Protection profiles for secure signature creation device — Part 2: Device with key generation;
- Protection profiles for secure signature creation device — Part 3: Device with key import;
- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application;
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application;
- Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application.

Preparation of this document as a protection profile (PP) follows the rules of the Common Criteria version 3.1 [2], [3] and [4].

Correspondence and comments to this protection profile about secure signature creation device with key import (PP SSCD KI) should be referred to:

CONTACT ADDRESS

CEN/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium

Tel **+32 2 550 0813**
Fax **+32 2 550 0966**

Email **isss@cenorm.be**

1 Scope

This European standard specifies a protection profile for a secure signature creation device with signing keys import possibility: SSCD with key import (SSCD KI).

2 Normative references

For the application of this European standard the following documents are indispensible:

EN 14169-1, Protection profiles for secure signature creation device — Part 1: Overview

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

3 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in EN 14169-1 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 3: Device with key import
Version:	1.0.2
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012-07-24
Registration:	BSI-CC-PP-0075
CC version:	3.1 Revision 3
Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final
Keywords:	secure signature creation device, electronic signature, digital signature, key import

4.2 PP overview

This Protection Profile is established by CEN as a European standard for products to create electronic signatures. It fulfils requirements of directive[1] 1999/93/ec of the European parliament and of the council of 13 December 1999 on *a community framework for electronic signatures*.

In accordance with article 9 of this European directive this standard can be indicated by the European commission in the Official Journal of the European Communities as generally recognised standard for electronic signature products.

This protection profile defines security functional requirements and security assurance requirements that comply with those defined in Annex III of **the directive** for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for this protection profile.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of **the directive** [1] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile (PP).

This Protection Profile describes core security requirements for a secure device that can import a signing key[2] (signature creation data, SCD) and operates to create electronic signatures with the imported key. A device evaluated according to this protection profile and used in the specified environments can be trusted to create any type of digital signature. As such this PP can be used for any device that has been configured to create a digital signature. Specifically this PP allows the qualification of a product as a device for creating an advanced electronic signature as defined in **the directive**.

The intent of this Protection Profile is to specify security functional and assurance requirements defined in **the directive** [1], Annex III for secure signature creation devices (SSCD), which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of **the directive** [1] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with this Protection Profile (PP).

This EN14169-3 “Protection profiles for secure signature creation device — Part 3: Device with key import” defines the core security requirements for SSCD importing signature creation data (SCD) and creating advanced electronic signature, which if based on valid qualified certificates are qualified electronic signatures. A SSCD, which fulfils only these core security requirements, may be used by the signatory in a secure environment for signature creation. The CSP will generate SCD/SVD pair in a secure environment and import the SCD into the SSCD so that it can be delivered to the signer with at least one SCD and possibly Certificate info stored in the SSCD. The TOE may implement additional security functions e.g. to support integrity protection of imported data to be signed. The related security requirements are not subject of this core PP but extended PP EN14169-6 “Protection profiles for secure signature creation device — Part 6: Device with key import and Trusted Communication with Signature creation application” will address them claiming conformance to this core PP.

The assurance level for this PP is EAL4 augmented with AVA_VAN.5.

---

1 This European directive is referred to in this PP as “the directive”.

2 An SSCD that can import SCD/SVD was defined in the previous version of this PP (CWA 14169) as a Type 2 SSCD. The notion of types does not exist anymore in this series of ENs. In order to refer to the same functionality, a reference to EN14169-3 (i.e. Part 3) should be used.

4.3 TOE overview

4.3.1 Operation of the TOE

This section presents a functional overview of the TOE in its distinct operational environments:

- The preparation environment, where the TOE interacts with a certification service provider (CSP) through a SCD/SVD generation application to import the signature creation data (SCD) and a certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding to the SCD the certification service provider has generated. The SCD/SVD generation application transmits the SVD to the CGA. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference authentication data (RAD).
- The signing environment where the TOE interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature[3].
- The management environments where the TOE interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The preparation environment, the signing environment and the management environment are secure and protect data exchanged with the TOE. Figure 3 in Part 1 [6] of this standard illustrates the operational environment.

The TOE stores signature creation data (SCD) and reference authentication data (RAD). The TOE may store multiple instances of SCD. In this case the TOE provides a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE may be used to create an advanced electronic signature as defined in Article 5.1 of **the directive**. Determining the state of the certificate as qualified is beyond the scope of this standard.

The signature creation application is assumed to protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash value required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm.

The TOE stores signatory reference authentication data (RAD) to authenticate a user as its signatory. The RAD is a password (e.g. PIN), a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE may provide a user interface to directly receive verification authentication data (VAD) from the user, alternatively, the TOE receive the VAD from the signature creation application (SCA). If the signature creation application handles, is requesting or obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

---

[3] At a pure functional level the SSCD creates a digital signature; for an implementation of the SSCD, in that meeting the requirements of this PP and with the key certificate created as specified in **the directive**, Annex I, the result of the signing process can be used as to create a qualified electronic signature.

A certification service provider and a SSCD-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions may include:

- initialising the RAD,
- generating a key pair,
- storing personal information of the legitimate user.

A typical example of an SSCD is a smart card. In this case a smart card terminal may be deployed that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on a personal computer connected to the card terminal. The signature creation application, after presenting the document to the user and after obtaining the authorization PIN, initiates the digital signature creation function of the smart card through the terminal.

4.3.2 Target of evaluation

The TOE is a combination of hardware and software configured to securely import, use and manage signature creation data (SCD). The SSCD protects the SCD during its lifecycle beginning with import as to be used in a signature creation process solely by its signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the digital signature.

The TOE provides the following functions:

(1) to import signature creation data (SCD) and, optionally, the correspondent signature verification data (SVD),
(2) to, optionally, receive and store certificate info,
(3) to switch the TOE from a non-operational state to an operational state, and
(4) if in an operational state, to create digital signatures for data with the following steps:
    (a) select a set of SCD if multiple sets are present in the SSCD,
    (b) authenticate the signatory and determine its intent to sign,
    (c) receive data to be signed or a unique representation thereof (DTBS/R),
    (d) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

The TOE may implement its function for digital signature creation to conform to the specifications in ETSI TS 101 733 (CAdES) [7], ETSI TS 101 903 (XAdES) [8] and ETSI TS 102 778 (PAdES) [9].

The TOE is prepared for the signatory's use by

(1) import at least one set of SCD, and
(2) personalising for the signatory by storing in the TOE:
    (a) the signatory’s reference authentication data (RAD)
    (b) optionally, certificate info for at least one SCD in the TOE.

After import the SCD is in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

After preparation the intended legitimate user should be informed of the signatory’s verification authentication data (VAD) required for use of the TOE in signing. If the VAD is a password or PIN, the means of providing this information is expected to protect the confidentiality and the integrity of the corresponding RAD.

If the use of an SCD is no longer required, then it should be destroyed (e.g. by erasing it from memory) as well as the associated certificate info, if any exists.

4.3.3 TOE lifecycle

4.3.3.1 General

The TOE lifecycle distinguishes stages for development, preparation and operational use. Please take note that other lifecycle definitions are possible; when this PP is claimed by other PPs (e.g. for a SSCD providing additionally trusted communications with the signature creation application).

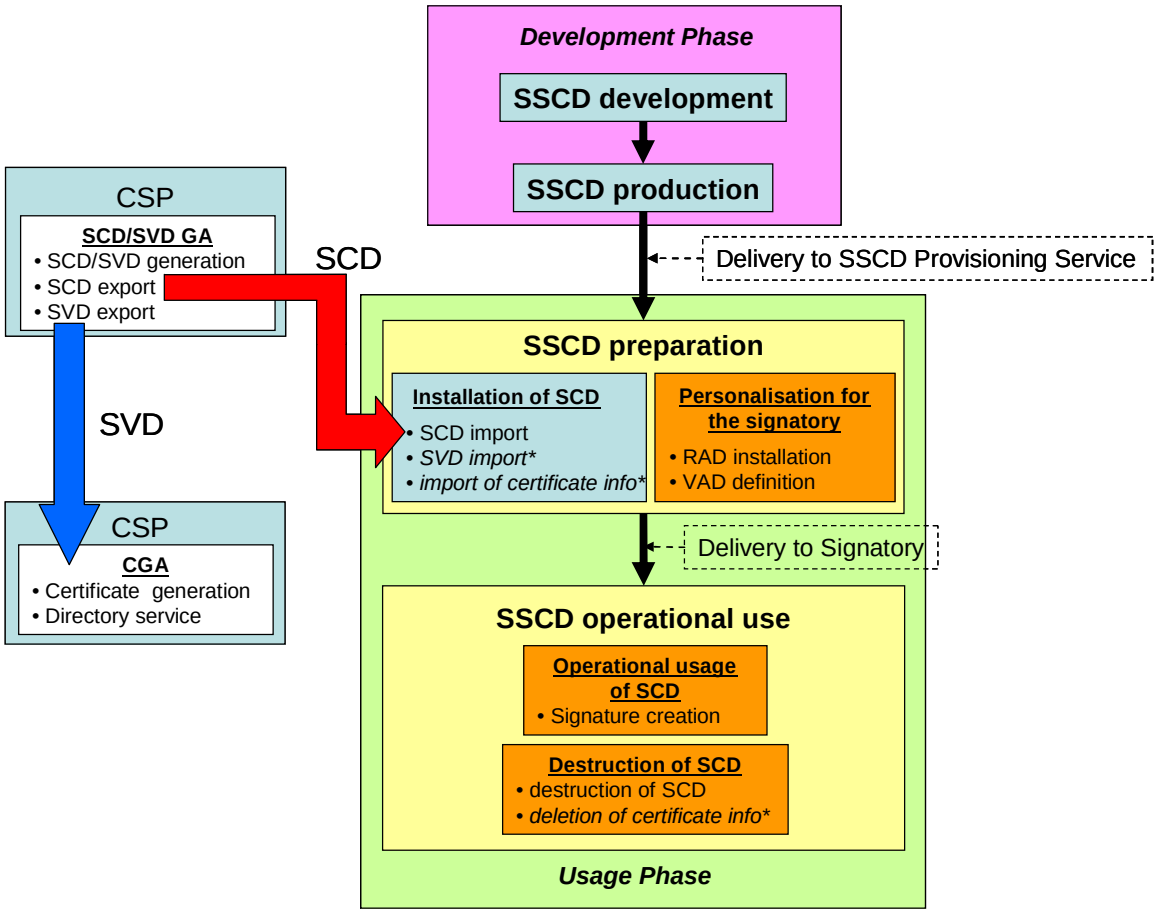


Figure 1: Example of TOE lifecycle[4]

The development phase comprises the development and production of the TOE. The development phase is subject of the evaluation according to the assurance lifecycle (ALC) class. The development phase ends with the delivery of the TOE to the SSCD-provisioning service.

[4]The asterisks * mark the optional import of the SVD and certificate info during TOE preparation and certificate info deletion when SCD is destroyed.

The operational usage of the TOE comprises the preparation stage and the operational use stage. The TOE operational use stage begins when the signatory has obtained both the VAD and the TOE. Enabling the TOE for signing requires at least one set of SCD stored in its memory.

Figure 1 shows an example of the lifecycle where an SCD or SCD/SVD pair is imported from SSCD-provisioning service before delivery to the signatory. The lifecycle may allow import of SCD or SCD/SVD key pairs after delivery to the signatory as well.

4.3.3.2 Preparation stage

The preparation phase of the TOE lifecycle is processing the TOE from the customer's acceptance of the delivered TOE to a state ready for operation by the signatory. The customer receiving the TOE from the manufacturer is the SSCD-provisioning service that prepares and provides the SSCD to subscribers. The preparation includes

(1) The personalization of the TOE for use by the signatory, i.e. the installation of the RAD in the TOE and handover of VAD to the signatory.

(2) The initialization of the TOE, i.e. the CSP generates the SCD/SVD pair by means of a SCD/SVD generation device, loads the SCD to the TOE, and sends the SVD to the CGA. The TOE may import and store the SCD/SVD pair.

(3) The generation of the (qualified) certificate containing among others (cf. [1], Annex II)
   (a) the SVD which correspond to SCD under the control of the signatory;
   (b) the name of the signatory or a pseudonym, which is to be identified as such,
   (c) an indication of the beginning and end of the period of validity of the certificate.

(4) The preparation may include optional loading of the certificate info into the SSCD for signatory convenience.

The CSP generates a SCD/SVD pair and imports SCD, and optionally also SVD, into the SSCD. The CSP ensures
(a) the correspondence between SCD and SVD,
(b) that algorithm and key size for the SVD are appropriate.

Please take note that verifying whether the claimed identity of the signer originates from that given SSCD has to be done by the CSP operating the CGA.

If the TOE is used for creation of advanced electronic signatures, the certificate links the signature verification data to the person (i.e. the signatory) and confirms the identity of that person (cf. [1], article 2, clause 9).

This PP requires the TOE to provide mechanisms for import of SCD, implementation of the SCD and personalization. The environment is assumed to protect all other processes for TOE preparation like SCD transfer between the SCD/SVD generation device and the TOE, and SVD transfer between the SCD/SVD generation device and the CGA. The CSP may export the SVD to the TOE for internal use by the TOE (e.g., self-test).

Before generating a (qualified) certificate, the CSP is expected to first store the SCD in a SSCD. A secure channel with the TOE may be used to support this, by ensuring integrity of the SCD during transmission to the TOE.

4.3.3.3 Operational use stage

In this lifecycle stage the signatory can use the TOE to create advanced electronic signatures.

The operational phase of the TOE starts when at least one SCD/SVD pair is generated by the CSP and the SCD is imported into the SSCD and when the signatory takes control over the TOE and makes the SCD operational. The signatory uses the TOE with a trustworthy SCA in a secured environment only. The SCA is assumed to protect the DTBS/R during the transmission to the TOE.

The signatory can also interact with the SSCD to perform management tasks, e.g. reset a RAD value or use counter if the password/PIN in the reference data has been lost or blocked. Such management tasks require a secure environment.

The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as SSCD.

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it will support further functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[5]. If the conditions to obtain a qualified certificate are met, the new key can also be used to create advanced electronic signatures. The optional TOE functions for additional key generation and certification may require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider in an environment that is secure.

The TOE life cycle as SSCD ends when all SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

5 Conformance claims

5.1 CC conformance claim

This PP uses the Common Criteria version 3.1 Revision 3 (see chapter 10).

This PP is conforming to Common Criteria Part 2 [3] extended.

This PP is conforming to Common Criteria Part 3 [4].

5.2 PP claim, Package claim

This PP does not claim conformance to any other PP.

This PP is conforming to assurance package EAL4 augmented with AVA_VAN.5 defined in CC part 3 [4].

[5] The certificate request in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory's existing SCD.

5.3 Conformance rationale

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

5.4 Conformance statement

This PP requires **strict** conformance of the ST or PP claiming conformance to this PP.

6 Security problem definition

6.1 Assets, users and threat agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

Assets and objects:

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

2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.

3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

Users and subjects acting for users:

1. User: End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

2. Administrator: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

3. Signatory: User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

Threat agents:

1. Attacker: Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

6.2 Threats

6.2.1 **T.SCD_Divulg** *Storing, copying and releasing of the signature creation data*

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

6.2.2 **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.

6.2.3 **T.Hack_Phys** *Physical attacks through the TOE interfaces*

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

6.2.4 **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.

6.2.5 **T.SigF_Misuse** *Misuse of the signature creation function of the TOE*

An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. 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.

6.2.6 **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 intended to sign.

6.2.7 **T.Sig_Forgery** *Forgery of the electronic signature*

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable 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.

6.3 Organisational security policies

6.3.1 **P.CSP_QCert** *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the directive**, article 2, clause 9, and Annex I) for the SVD. 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 as SSCD is evident with signatures through the certificate or other publicly available information.

6.3.2 **P.QSign** *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[6]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory 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.

6.3.3 **P.Sigy_SSCD** *TOE as secure signature creation device*

The TOE meets the requirements for an SSCD laid down in Annex III of **the directive** [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.

6.3.4 **P.Sig_Non-Repud** *Non-repudiation of signatures*

The lifecycle of the SSCD, 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.

6.4 Assumptions

6.4.1 **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.

6.4.2 **A.SCA** *Trustworthy signature creation application*

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

6.4.3 **A.CSP** *Secure SCD/SVD management by CSP*

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

7 Security objectives

7.1 Security objectives for the TOE

7.1.1 **Relation to PP SSCD KG**

[6] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

Security objectives for the TOE in this PP, which are identically stated in the PP SSCD KG, are OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID and OT.Tamper_Resistance (these are independent from the fact whether SCD are imported from the operational environment or generated by the TOE itself).

The remaining security objective for the TOE OT.SCD_Auth_Imp is related to SCD import only and is therefore not present in PP SSCD KG.

The following security objectives for the TOE of the PP SSCD KG, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique and OT.SCD_SVD_Corresp are not needed for the TOE in this PP because the SCD/SVD generation takes place outside of the TOE (see also chap. 7.2.1).

7.1.2 **OT.Lifecycle_Security** *Lifecycle security*

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Application note 1: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD import. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.

7.1.3 **OT.SCD_Auth_Imp** *Authorized SCD import*

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

7.1.4 **OT.SCD_Secrecy** *Secrecy of the signature creation data*

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Application note 2: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD import, signature creation operation, storage and secure destruction.

7.1.5 **OT.Sig_Secure** *Cryptographic security of the electronic signature*

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

7.1.6 **OT.Sigy_SigF** *Signature creation function for the legitimate signatory only*

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

7.1.7 **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.

7.1.8 **OT.EMSEC_Design** *Provide physical emanations security*

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

7.1.9 **OT.Tamper_ID** *Tamper detection*

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

7.1.10 **OT.Tamper_Resistance** *Tamper resistance*

The TOE shall prevent or resist physical tampering with specified system devices and components.

7.2 Security objectives for the operational environment

7.2.1 Relation to PP SSCD KG

Security objectives for the operational environment in this PP, which are identically stated in the PP SSCD KG, are OE.SVD_Auth, OE.CGA_QCert, OE.SSCD_Prov_Service, OE.HID_VAD, OE.DTBS_Intend, OE.DTBS_Protect and OE.Signatory (these are independent from the fact whether SCD are imported from the operational environment or generated by the TOE itself).

The remaining four security objectives OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique and OE.SCD_SVD_Corresp stated in this PP are not present in PP SSCD KG, as these do only apply if the TOE supports key import.

7.2.2 **OE.SCD/SVD_Auth_Gen** *Authorized SCD/SVD generation*

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

7.2.3 **OE.SCD_Secrecy** *SCD Secrecy*

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

7.2.4 **OE.SCD_Unique** *Uniqueness of the signature creation data*

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

7.2.5 **OE.SCD_SVD_Corresp** *Correspondence between SVD and SCD*

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD send to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

7.2.6 **OE.SVD_Auth** *Authenticity of the SVD*

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

7.2.7 **OE.CGA_Qcert** *Generation of qualified certificates*

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

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,

(c) the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

7.2.8 **OE.SSCD_Prov_Service** *Authentic SSCD provided by SSCD-provisioning service*

The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

7.2.9 **OE.HID_VAD** *Protection of the VAD*

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

7.2.10 **OE.DTBS_Intend** *SCA sends data intended to be signed*

The signatory shall use a trustworthy SCA that

(a) 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,

(b) sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,

(c) attaches the signature produced by the TOE to the data or provides it separately.

Application note 3: 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.

7.2.11 **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.

7.2.12 **OE.Signatory** *Security obligation of the signatory*

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

7.3 Security objectives rationale

7.3.1 Security objectives backtracking

Table 1 Mapping of security problem definition to security objectives

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_Qcert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg		X	X							X	X									
T.SCD_Derive				X								X								
T.Hack_Phys			X				X	X	X											
T.SVD_Forgery													X		X					
T.SigF_Misuse	X				X	X											X	X	X	X
T.DTBS_Forgery						X												X	X	
T.Sig_Forgery				X								X		X						
P.CSP_Qcert	X	X								X			X	X						
P.Qsign				X	X									X				X		
P.Sigy_SSCD	X	X	X	X	X	X	X		X	X	X	X				X				
P.Sig_Non-Repud	X		X	X	X	X	X	X	X		X	X	X	X	X	X		X	X	X
A.CGA														X	X					
A.SCA																		X		
A.CSP										X	X	X	X							

7.3.2 Security objectives sufficiency

Countering of threats by security objectives:

T.SCD_Divulg (Storing, copying and releasing of the signature creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in **the directive** [1], recital (18). This threat is countered by

- OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment, and
- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

T.SCD_Derive (Derive the signature creation data) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD given to the CGA for certificate generation. T.SVD_Forgery is addressed by

- OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD, and
- OE.SVD_Auth, which ensures the authenticity of the SVD given to the CGA of the CSP.

T.SigF_Misuse (Misuse of the signature creation function of the TOE) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by **the directive** [1], Annex III, paragraph 1, literal (c). OT.Lifecycle_Security, (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD on demand of the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) 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. If the SCA provides the human interface for the user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. **OE.Signatory** ensures also that the signatory keep their VAD confidential.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of

- OE.DTBS_Intend, which ensures that the SCA sends only those DTBS intended to be signed by the signatory, and

- 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.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OE.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OE.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

Enforcement of OSPs by security objectives:

P.CSP_QCert (CSP generates qualified certificates) establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet the Annex II of **the directive** [1]. This is ensured as follows

- OE.SCD_Unique meets the paragraph 1(a) of **the directive** [1], Annex III, by the requirements that the SCD used for signature creation can practically occur only once.
- OE.SCD_Unique, OT.SCD_Secrecy and OE.SCD_Secrecy meet the paragraph 1(a) of **the directive** [1], Annex III, by the requirements to ensure the secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of SCD against specific attacks.

- OT.SCD_Secrecy and OT.Sig_Secure meet the paragraph 1(b) of **the directive** [1], Annex III, by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE.
- OT.Sigy_SigF and OE.SCD_Secrecy meet the paragraph 1(c) of **the directive** [1], Annex III, by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others.
- OT.DTBS_Integrity_TOE meets the requirements the paragraph 2 of **the directive** [1], Annex III, The TOE must not alter the DTBS/R.

Please take note, the requirements of **the directive** [1], Annex III, 2., that the SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send them to the SSCD for signing.

The usage of SCD under sole control of the signatory sole control is ensured by

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- OT.SCD_Auth_Imp, which limits SCD import to authorised users only,
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation.
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service.

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented 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.

OE.SSCD_Prov_Service ensures that the signatory uses an authentic copy of the TOE, initialised and personalised for the signatory.

OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment. OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.SCD_SVD_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD of the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE under sole control of the signatory.

OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

Upkeep of assumptions by security objectives:

A.SCA (Trustworthy signature creation application) 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.CGA (Trustworthy certificate generation application) 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 (CGA proves the authenticity of the SVD), which ensures the verification of the authenticity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.CSP (Secure SCD/SVD management by CSP) establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

8 Extended components definition

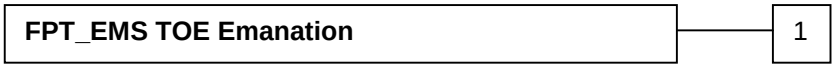
The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN Security audit data generation is included in a PP or ST using FPT_EMS.1.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to [*assignment: list of types of TSF data*] and [*assignment: list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [*assignment: type of users*] are unable to use the following interface [*assignment: type of connection*] to gain access to [*assignment: list of types of TSF data*] and [*assignment: list of types of user data*].

9 Security requirements

9.1 Security functional requirements

9.1.1 Use of requirement specifications

The Common Criteria allow several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration.* Each of these operations is used in this PP. Operations not performed in this PP are identified in order to enable instantiation of the PP into a Security Target (ST).

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word “refinement” in **bold** text and the added or changed words are in bold text, or (ii) included in text as **bold** text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed or the removed words are simply striked through (e.g., like in ~~removed words~~).

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections 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*.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing as underlined text denotes assignments, which have been made by the PP authors, and the original text of the component is given by a footnote. 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*.

An **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. (Please take note that the requirements FDP_ITC.1/SCD, FDP_UCT.1/SCD and FTP_ITC.1/SCD are marked this way although they are not iterated in this PP. This is due to the fact that consistent naming was desired to “ Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application” in which FDP_ITC.1, FDP_UCT.1 and FTP_ITC.1 are iterated.)

9.1.2 Cryptographic support (FCS)

9.1.2.1 **FCS_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components.

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

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

Application note 4: The ST writer shall perform the missing operations in the element FCS_CKM.4.1. The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid any more.

9.1.2.2 **FCS_COP.1 Cryptographic operation**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform digital signature creation[7] in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application note 5: The ST writer shall perform the missing operations in the element FCS_COP.1.1. The ST writer should consult the notified body or the certification body for the admissible algorithms, cryptographic key sizes and other parameters for algorithms, and standards for digital signature creation by SSCD. The operations in the element FCS_COP.1.1 shall be appropriate for the SCD imported according to FTP_ICT.1/SCD.

9.1.3 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Table 2 Subjects and security attributes for access control

Subject or object the security attribute is associated with	**Security attribute type**	**Value of the security attribute**
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes

Application note 6: The writer of PP or ST may define additional objects and security attributes.

[7] [assignment: *list of cryptographic operations*]

9.1.3.1 **FDP_ACC.1/SCD_Import Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD_Import: The TSF shall enforce the SCD Import SFP[8] on
(1) subjects: S.User,
(2) objects: SCD,
(3) operations: import of SCD[9].

9.1.3.2 **FDP_ACF.1/SCD_Import Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SCD_Import: The TSF shall enforce the SCD Import SFP[10] to objects based on the following: the S.User is associated with the security attribute "SCD/SVD Management"[11].

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

S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD[12].

FDP_ACF.1.3/ SCD_Import: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[13].

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

S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD[14].

---

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

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

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

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

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

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

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

9.1.3.3 **FDP_ACC.1/Signature_Creation Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Signature_Creation: The TSF shall enforce the Signature Creation SFP[15] on
(1) subjects: S.User,
(2) objects: DTBS/R, SCD,
(3) operations: signature creation[16].

9.1.3.4 **FDP_ACF.1/Signature_Creation Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature_Creation: The TSF shall enforce the Signature Creation SFP[17] to objects based on the following:
(1) the S.User is associated with the security attribute "Role" and
(2) the SCD with the security attribute "SCD Operational"[18].

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

R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[19].

FDP_ACF.1.3/ Signature_Creation: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[20].

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

S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[21].

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

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

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

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

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

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

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

9.1.3.5 **FDP_ITC.1/SCD Import of user data without security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/SCD The TSF shall enforce the SCD Import SFP[22] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SCD The TSF shall ignore any security attributes associated with the ~~user data~~ **SCD** when imported from outside the TOE.

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

9.1.3.6 **FDP_UCT.1/SCD Basic data exchange confidentiality**

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1/SCD The TSF shall enforce the SCD Import SFP[23] to receive[24] ~~user data~~ **SCD** in a manner protected from unauthorised disclosure.

Application note 7: The component FDP_UCT.1/SCD requires the TSF to ensure the confidentiality of the SCD during import. The refinement substituting “user data” by “SCD” highlights that confidentiality of other imported user data like DTBS is not required.

9.1.3.7 **FDP_RIP.1 Subset residual information protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[25] the following objects: SCD[26].

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

1. SCD

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

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

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

[25] [selection: *allocation of the resource to, deallocation of the resource from*]

[26] [assignment: *list of objects*]

2. SVD (if persistent stored by TOE).

The DTBS/R temporarily stored by TOE has the user data attribute "integrity checked stored data":

9.1.3.8 **FDP_SDI.2/Persistent Stored data integrity monitoring and action**

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/Persistent The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[27] on all objects, based on the following attributes: integrity checked persistent stored data[28].

FDP_SDI.2.2/Persistent 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[29].

9.1.3.9 **FDP_SDI.2/DTBS Stored data integrity monitoring and action**

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[30] on all objects, based on the following attributes: integrity checked stored DTBS[31].

FDP_SDI.2.2/DTBS 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[32].

Application note 8: The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

9.1.4 Identification and authentication (FIA)

9.1.4.1 **FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow
(1) Self-test according to FPT_TST.1,

[27] [assignment: *integrity errors*]
[28] [assignment: *user data attributes*]
[29] [assignment: *action to be taken*]
[30] [assignment: *integrity errors*]
[31] [assignment: *user data attributes*]
[32] [assignment: *action to be taken*]

(2) [assignment: *list of additional TSF-mediated actions*][33]
on behalf of the user to be performed before the user is identified.

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

Application note 9: The ST writer shall perform the missing operation in the element FIA_UID.1.1. The list of additional TSF-mediated actions may be empty (i.e. assignment "none") or include TSF-mediated actions like establishing a trusted path between the user using the HI of an external device. The TOE may identify the user by default or by selection of the role and RAD against the authentication will be performed. Identification by default is normally linked to the TOE lifecycle, e.g. the TOE may identify by default the Administrator before the signatory's RAD is created and the signatory if signatory's RAD exists. In case of multi-application smart cards (i.e. the smart card provides more than the signature creation application) the user identifies themselves as signatory by selection of the signature application directory file and therefore the PIN authentication will be performed against the signatory PIN. The user may identify themselves as Administrator by selection of an authentication key as Administrator and therefore authentication will be performed by external authenticate or mutual device authentication.

9.1.4.2 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow
(1) Self-test according to FPT_TST.1,
(2) Identification of the user by means of TSF required by FIA_UID.1.
(3) [assignment: *list of additional TSF-mediated actions*][34]
on behalf of the user to be performed before the user is authenticated.

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

Application note 10: The ST writer shall perform the missing operation in the element FIA_UAU.1.1. The list of additional TSF-mediated actions may be empty (i.e. assignment "none") or include TSF-mediated actions like establishing a trusted path between the user using the HI of an external device.

9.1.4.3 **FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[35].

[33] [assignment: *list of TSF-mediated actions*]

[34] [assignment: *list of TSF mediated actions*]

[35] [assignment: *list of authentication events*]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[36], the TSF shall block RAD[37].

Application note 11: The ST writer shall perform the missing operation in the element FIA_AFL.1.1. The assignment shall be consistent with the implemented authentication mechanism and the resistant against attacks with high attack potential.

9.1.5 Security management (FMT)

9.1.5.1 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy[38].

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

9.1.5.2 **FMT_SMF.1 Security management functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
(1) Creation and modification of RAD,
(2) Enabling the signature creation function,
(3) Modification of the security attribute SCD/SVD management, SCD operational,
(4) [assignment: *list of other security management functions to be provided by the TSF*][39].

Application note 12: The ST writer shall perform the missing operation in the element FMT_SMF.1.1. The list of other security management functions to be provided by the TSF may be empty (i.e. assignment "none").

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

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

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

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

9.1.5.3 **FMT_MOF.1 Management of security functions behaviour**

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to enable[40] the functions signature creation function[41] to R.Sigy[42].

9.1.5.4 **FMT_MSA.1/Admin Management of security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin The TSF shall enforce the SCD Import SFP[43] to restrict the ability to modify [*assignment: other operations*][44] the security attributes SCD/SVD management[45] to R.Admin[46].

9.1.5.5 **FMT_MSA.1/Signatory Management of security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Signatory The TSF shall enforce the Signature Creation SFP[47] to restrict the ability to modify[48] the security attributes SCD operational[49] to R.Sigy[50].

---

[40] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[41] [assignment: *list of functions*]

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

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

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

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

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

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

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

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

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

9.1.5.6 **FMT_MSA.2 Secure security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[51].

Application note 13: The ST writer shall define which values of the security attribute SCD/SVD Management are secure for the TOE and the intended TOE lifecycle. E.g. if the TOE supports generation of SCD/SVD pairs by the signatory and a trusted channel for export of the SVD to the CGA then the subject S.Sigy may or may not be assigned the security attribute SCD/SVD Management to "yes". If the TOE supports the generation of the SCD/SVD pair in the preparation phase in secure environment only the TSF should enforce the assignment of the security attribute SCD/SVD Management of S.Admin to "yes" and of S.Sigy to "no".

9.1.5.7 **FMT_MSA.3 Static attribute initialisation**

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the SCD Import SFP and Signature Creation SFP[52] to provide restrictive[53] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the R.Admin[54] to specify alternative initial values to override the default values when an object or information is created.

9.1.5.8 **FMT_MSA.4 Security attribute value inheritance**

Hierarchical to: No other components.

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

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

(1) If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.

(2) If S.Admin imports SCD while S.Sigy is currently authenticated, the

[51] [selection: *list of security attributes*]

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

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

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

security attribute “SCD operational” of the SCD shall be set to “yes” after import of the SCD as a single operation.[55]

9.1.5.9 **FMT_MTD.1/Admin Management of TSF data**

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

FMT_MTD.1.1/Admin The TSF shall restrict the ability to create[56] the RAD[57] to R.Admin[58].

9.1.5.10 **FMT_MTD.1/Signatory Management of TSF data**

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

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to modify [*assignment: other operations*] [59] the RAD[60] to R.Sigy[61].

Application note 14: The ST writer shall perform the missing operation in the element FMT_MTD.1.1. The missing assignment may be “none”.

9.1.6 Protection of the TSF (FPT)

9.1.6.1 **FPT_EMS.1 TOE Emanation**

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

FPT_EMS.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [*assignment: specified limits*] enabling access to RAD[62] and SCD[63].

---

[55] [assignment: *rules for setting the values of security attributes*]

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

[57] [assignment: *list of TSF data*]

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

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

[60] [assignment: *list of TSF data*]

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

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

[63] [assignment*: list of types of user data*]

FPT_EMS.1.2 The TSF shall ensure [*assignment: type of users*] are unable to use the following interface [*assignment: type of connection*] to gain access to RAD[64] and SCD[65].

Application note 15: The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.
Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

9.1.6.2 **FPT_FLS.1 Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
(1) self-test according to FPT_TST fails,
(2) [assignment*: list of other types of failures in the TSF*][66].

Application note 16: The ST writer shall perform the missing assignment in the element FPT_FLS.1.1. The assignment (1) addresses failures detected by a failed self-test and requiring appropriate action to prevent security violation. When the TOE is in a secure state the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.

9.1.6.3 **FPT_PHP.1 Passive detection of physical attack**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

[65] [assignment*: list of types of user data*]

[66] [assignment*: list of types of failures in the TSF*]

9.1.6.4 **FPT_PHP.3 Resistance to physical attack**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application note 17: The TOE will implement appropriate measures to continuously counter physical tampering which may compromise the SCD. The "automatic response" in the element FPT_PHP.3.1 means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Due to the nature of these attacks the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). But physical tampering must not reveal information of the SCD. E.g. the TOE may be physically tampered in power-off state of the TOE (e.g. a smart card), which does not allow TSF for overwriting the SCD but leads to physical destruction of the memory and all information therein about the SCD. In case of physical tampering the TFS may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1 requires the TSF to react on physical tampering in a way that the signatory is able to determine whether the TOE was physical tampered or not. E.g. the TSF may provide an appropriate message during start-up or the guidance documentation may describe an failure of TOE start-up as indication of physical tampering.

9.1.6.5 **FPT_TST.1 TSF testing**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions] [assignment: conditions under which self-test should occur*] to demonstrate the correct operation of the TSF[67].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[68].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of TSF[69].

Application note 18: The ST writer shall perform the operations in the element FPT_TST.1.1. The component FPT_TST.1 addresses only the self-test of the TSF or part of the TSF. If the TSF relays on security feature of the hardware platform of part of the TOE the ST should consider inclusion FPT_TEE.1 to require the TSF to test these features for correct work of the dependent TSF.

9.1.6.6 **FTP_ITC.1/SCD Inter-TSF trusted channel**

---

[67] [selection: *[assignment: parts of TSF], the TSF*]

[68] [selection: *[assignment: parts of TSF data], TSF data*]

[69] [selection: *[assignment: parts of TSF], TSF*]

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SCD 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/SCD The TSF shall permit another trusted IT product[70] to initiate communication via the trusted channel.

FTP_ITC.1.3/SCD The TSF shall initiate communication via the trusted channel for
(1) Data exchange integrity according to FDP_UCT.1/SCD,
(2) [assignment: *list of other functions for which a trusted channel is required*][71].

Application note 19: The component FPT_ITC.1 requires the TSF to support a trusted channel established to another trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD. The ST writer shall perform the missing operations in the element FTP_ITC.1.3/SCD. If the TSF does not enforce the use of trusted channel for other functions the operation in the element FTP_ITC.1.3/SCD is “none”.

9.2 Security assurance requirements

Table 3 Assurance Requirements: EAL4 augmented with AVA_VAN.5

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

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

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

9.3 Security requirements rationale

9.3.1 Security requirement coverage

Table 4 Mapping of functional requirements to security objectives for the TOE

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.4	X		X						
FCS_COP.1	X			X					
FDP_ACC.1/SCD_Import	X	X							
FDP_ACC.1/Signature_Creation	X				X				
FDP_AFC.1/SCD_Import	X	X							
FDP_AFC.1/Signature_Creation	X				X				
FDP_ITC.1/SCD	X								
FDP_UCT.1/SCD	X		X						
FDP_RIP.1			X		X				
FDP_SDI.2/Persistent			X	X					
FDP_SDI.2/DTBS					X	X			
FIA_AFL.1					X				
FIA_UAU.1		X			X				
FIA_UID.1		X			X				
FMT_MOF.1	X				X				
FMT_MSA.1/Admin	X								
FMT_MSA.1/Signatory	X				X				
FMT_MSA.2	X				X				
FMT_MSA.3	X				X				
FMT_MSA.4	X				X				

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FMT_MTD.1/Admin	X				X				
FMT_MTD.1/Signatory	X				X				
FMT_SMR.1	X				X				
FMT_SMF.1	X				X				
FPT_EMS.1			X				X		
FPT_FLS.1			X						
FPT_PHP.1								X	
FPT_PHP.3			X						X
FPT_TST.1	X		X	X					
FTP_ITC.1/SCD	X		X						

9.3.2 Security functional requirements sufficiency

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR as follows.

The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ICT.1/SCD.

The secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is controlled by access control FDP_ACC.1/Signature_Creation, FDP_AFC.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.4 ensures a secure SCD destruction.

OT.SCD_Auth_Imp (Authorized SCD import) is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FDP_UCT.1/SCD and FTP_ICT.1/SCD ensures the confidentiality for SCD import.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

The SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensure the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is provided by SFR for identification authentication and access control.

The FIA_UAU.1 and FIA_UID.1 that ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. The SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS.

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. FMT_MOF.1 ensures that only the signatory can enable/disable the signature creation function. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

Furthermore, the security functionality specified by FDP_RIP.1 will ensure that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD have been deleted by the legitimate signatory.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered by the TOE. The verification that the DTBS/R has not been altered by the TOE is provided by integrity functions specified by FDP_SDI.2/DTBS.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

9.3.3 Satisfaction of dependencies of security requirements

Table 5 Satisfaction of dependencies of security functional requirements

Functional requirement	Dependencies	Satisfied by
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/SCD
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FDP_ITC.1/SCD, FCS_CKM.4
FDP_ACC.1/SCD_Import	FDP_ACF.1	FDP_ACF.1/SCD_Import
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/SCD_Import	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FPT_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_MSA.1	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory

Functional requirement	Dependencies	Satisfied by
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD_Import, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	No dependencies	n/a
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/SCD	No dependencies	n/a

Table 6 Satisfaction of dependencies of security assurance requirements

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

9.3.4 Rationale for chosen security assurance requirements

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to

high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

10 References

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

[5] Protection Profile Secure Signature Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002, also short SSCD-PP or CWA14169

[6] CEN prEN 14169-1:2010 Protection profiles for secure signature creation device — Part 1: Overview, date 2012-01

[7] ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp

[8] ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp

[9] ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp