CEN/TC 224

Date: 2009-12

prEN 14169-1:2009

CEN/TC 224

Secretariat: AFNOR

Protection profiles for Secure signature creation device — Part 2: Device with key generation

Schutzprofile Sichere Signaturerstellungseinheit — Teil 2: Gerät mit Schlüsselerzeugung

Dispositif sécurisé de signature électronique - Partie 2: Dispositif avec génération de clé

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage: Working Document
Document language: E

WD1 EN_14169_(E) vs100.doc

Contents

Page

Foreword

This document (prEN 14169-3:2009) 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.

0 Introduction

This European standard specifying a Protection Profile for a Secure Signature-Creation Device with key generation 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 C on the protection profile secure signature-creation devices, "EAL 4+".

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities. This protection profile describes core security requirements on secure signature-creation devices according to [1], Annex III.

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 secure signature-creation device protection profile (PP SSCD with key generation) 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

0.1 Document structure

Sections 1 to 4 provide the introductory material for this Protection Profile to be published as a European standard.

Section 5 provides the introductory material for the Protection Profile including the general purpose and TOE description.

Section 6 provides the CC conformance claim.

Section 7 provides a discussion of the security problem definition for expected TOE operational environment. This section defines the threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls. It defines also security policies to follow and assumptions about the operational environment.

Section 8 defines the security objectives for both the TOE and the TOE environment.

Section 9 contains the extended component definition for FPT_EMSEC.1.

Section 10 provides the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], which must be satisfied by the TOE.

Section 11 provides a rationale to explicitly demonstrate that the security objectives satisfy the security problem definition as described by organisational security policies, threats and assumptions.

Arguments are provided for the coverage of each organisational security policy, threat and assumption.

A bibliography is provided to identify background material.

1 Scope

This European standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: SSCD with key generation.

2 Normative references

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

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 Conventions and Terminology

3.1 Conventions

This document is drafted in accordance with the CEM/CENELEC directive and the content and structure of this document follow the rules and conventions laid out in Common Criteria 3.1.

Normative aspects of content in this European standard is specified according to the common criteria rules and not specifically identified by the verbs "*shall*" or "*must*".

3.2 Terms and definitions

For the purpose of this European standard the following terms are defined:

3.2.1 Legislative references

This European standard reflects the requirement of a European directive in the technical terms of a protection profile. The following terms are used in the text to reference the directive:

3.2.1.1
The Directive
Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on *"a Community framework for electronic signatures"* [1],

Note 1: References in this document to a specific article and paragraph of this directive are of the form "(**The Directive:** n.m)".

3.2.1.2
Annex
one of the annexes, Annex I, Annex II or Annex ||| of **The Directive**

3.2.2 Security Evaluation Terms

3.2.2.1
Common Criteria
CC
set of rules and procedures for evaluating the security properties of a product

Note: see bibliography for details on the specification of Common Criteria.

3.2.2.2
Evaluation Assurance Level
EAL
a set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria

3.2.2.3
Protection Profile
PP
document specifying security requirements for a class of products that conforms in structure and content to rules specified by common criteria

3.2.2.4
Security Target
ST
document specifying security requirements for a particular products that conforms in structure and content to rules specified by common criteria, which may be based on one or more Protection Profiles

3.2.2.5
Target of Evaluation
TOE
abstract reference in a document, such as a Protection Profile, for a particular product that meets specific security requirements

3.2.2.6
TOE Security Functions
TSF
functions implemented by the TOE to meet the requirements specified for it in a Protection Profile or Security Target

3.2.3 Technical terms

3.2.3.1
Administrator
user who performs TOE initialisation, TOE personalisation, or other TOE administrative functions

3.2.3.2
Advanced electronic signature
digital signature which meets specific requirements in **The Directive** (**The Directive:** 2.2)

*Note: according to **The Directive** a digital signature qualifies as an electronic signature if it:*

- *is uniquely linked to the signatory;*

- *is capable of identifying the signatory;*
- *is created using means that the signatory can maintain under his sole control, and*
- *is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.*

3.2.3.3
Authentication data
information used to verify the claimed identity of a user

3.2.3.4
Certificate
digital signature used as electronic attestation binding an SVD to a person confirming the identity of that person as legitimate signer (**The Directive: 2.9**)

3.2.3.5
Certificate info
information associated with a SCD/SVD pair that may be stored in a secure signature creation device

Note: Certificate info is either

- *a signer's public key certificate or,*
- *one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values.*

Certificate info may be combined with information to allow the user to distinguish between several certificates.

3.2.3.6
Certificate-generation application
CGA
collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate

3.2.3.7
Certification service provider
CSP
entity that issues certificates or provides other services related to electronic signatures (**The Directive:** 2.11)

3.2.3.8
Data to be signed
DTBS
all electronic data to be signed including a user message and signature attributes

3.2.3.9
Data to be signed or its unique representation
DTBS/R
data received by a secure signature creation device as input in a single signature-creation operation

Note: DTBS/R is either

- *a hash-value of the data to be signed (DTBS), or*
- *an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or*
- *the DTBS.*

3.2.3.10
Legitimate user
user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory

3.2.3.11
Notified body
organizational entity designated by a member state of the European Union as responsible for accreditation and

supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (**The Directive:** 1.1b and 3.4)

3.2.3.12
Qualified certificate

public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in **Annex II** (**The Directive:** 2.10)

3.2.3.13
Qualified electronic signature

advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate (**The Directive:** 5.1)

3.2.3.14
Reference authentication data
RAD

data persistently stored by the TOE for authentication of a user as authorised for a particular role

3.2.3.15
Secure signature-creation device
SSCD

personalized device that meets the requirements laid down in Annex III by being evaluated according to a security target conforming to this PP (**The Directive:** 2.5 and 2.6)

3.2.3.16
Signatory

legitimate user of an SSCD associated with it in the certificate of the signature-verification and who is authorized by the SSCD to operate the signature-creation function (**The Directive:** 2.3)

3.2.3.17
Signature attributes

additional information that is signed together with a user message

3.2.3.18
Signature-creation application
SCA

application complementing an SSCD with a user interface with the purpose to create an electronic signature

> *Note: A signature creation application is software consisting of a collection of application components configured to:*
>
> - *present the data to be signed (DTBS) for review by the signatory,*
> - *obtain prior to the signature process a decision by the signatory,*
> - *if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE*
> - *process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.*

3.2.3.19
Signature-creation data
SCD
private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature (**The Directive:** 2.4)

3.2.3.20
Signature-creation system
SCS
complete system that creates an electronic signature consists of the SCA and the SSCD

3.2.3.21
Signature-verification data
SVD
public cryptographic key that can be used to verify an electronic signature (**The Directive** 2.7)

3.2.3.22
SSCD-provisioning service
service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD

3.2.3.23
User
entity (human user or external IT entity) outside the TOE that interacts with the TOE

3.2.3.24
User Message
data determined by the signatory as the correct input for signing

3.2.3.25
Verification authentication data
VAD
data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics

4 Symbols and abbreviated terms

CC	Common Criteria
CGA	Certification generation application
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
RAD	Reference authentication data
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system

SDO	Signed data object
SFP	Security Function Policy
SSCD	Secure signature-creation device
ST	Security Target
SVD	Signature-verification data
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAD	Verification authentication data

5 Protection Profile Introduction

5.1 Overview of this section

This section provides document management and overview information. Section 5.2 “Protection Profile Reference” gives the label and further descriptive information necessary to enter this Protection Profile in a register. Section 5.3 “Protection Profile Overview” presents the purpose of this protection profile in the context of additional protection profiles for extended security requirements. This section is intended to be used as independent abstract, e.g. for use in a PP register. Section 5.4 “TOE Overview” provides an informal description of the functions of the TOE and summarizes the security requirements. That section is further intended for implementers as the basis for the informal description part in CC documents based on this PP.

5.2 Protection Profile Reference

Title:	Protection profiles for Secure signature creation device — Part 2: Device with key generation
Version:	1.03
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	(TBD)
Registration:	BSI-CC-PP-0059
CC version:	3.1 Revision 3
Editor:	Wolfgang Killmann, T-System GEI GmbH
General status:	final version for certification
Keywords:	secure signature-creation device, electronic signature, digital signature

5.3 Protection Profile 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.

[1] This European directive is referred to in this PP as “The Directive”.

This protection profile formally specifies the security-functional and assurance requirements 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.

For an electronic signature product that has been evaluated according to Common Criteria (version 3.1) as conforming to a Security Target (ST) that is compliant with this Protection Profile (PP) this European standard implies that European-Union Member States shall presume compliance with the requirements in Annex III of **The Directive** for that product.

This Protection Profile describes core security requirements for a secure device that can generate a signing key[2] (signature-creation-data, SCD) and operates to create electronic signatures with the generated 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**.

After an SSCD has generated a signing key, the corresponding public key (signature verification data, SVD) has to be provided as input to a certificate generating application (CGA). Security requirements for export of the SVD are described in a protection profile that extends this PP (EN14169-3 "*Protection Profiles for Secure signature creation device - Part 3: Device with key generation and trusted channel between SSCD and CGA*") and not in this document.

When operated in a secure environment for signature creation a signer may use an SSCD that fulfils only these core security requirements to create an advanced electronic signature.[3] Security requirements for an SSCD used in other environments are described in a separate protection profile that extend this PP (EN14169-4 "*Protection Profiles for Secure signature creation device - Part 4: Device with key generation and trusted channel between SSCD and SCA"*) and not in this document.

These extended Protection Profiles claim conformance to this PP[4].

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

5.4 TOE Overview

5.4.1 Operation of the TOE

Summarised in figure 1 this section presents a functional overview of the TOE in its distinct operational environments:

- The signing environment where it 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, or a unique representation thereof (DTBS/R) as input to the TOE signature-creation function and obtains the resulting digital signature[5].
- The preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The initialization

[2] An SSCD that can create its own SCD/SVD is known as an SSCD Type 3 to be distinguished from type 1 and type 2 as defined in the previous version of this PP (CWI 14160). The protection profile for a SSCD type 2 is in "EN14169-2 *Protection Profile Secure signature creation device - Part 2: Device with import of key*"

[3] An advanced electronic signature is defined as a digital signature created by an SSCD using a public key with a public key certificate created as specified in **The Directive**

[4] See CC part 1 chapter 8.5

[5] 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.

environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD).

- The management environments where it 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 signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE.

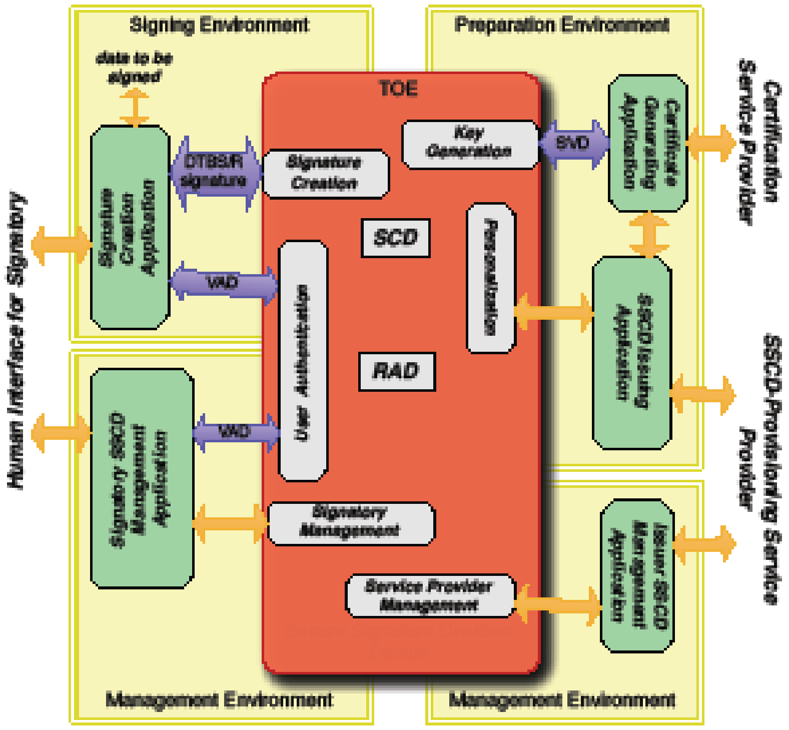
Signing Environment
Preparation Environment
data to be signed
TOE
Key Generation
SVD
DTBS/R signature
Signature Creation
Certificate Generating Application
Certification Service Provider
Human Interface for Signatory
Signature Creation Application
SCD
Personalization
VAD
User Authentication
SSCD Issuing Application
RAD
SSCD-Provisioning Service Provider
Signatory SSCD Management Application
VAD
Signatory Management
Service Provider Management
Issuer SSCD Management Application
Management Environment
Management Environment

Figure 1: Principal SSCD functions and operational environments

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE shall provide 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 of the SCD and restricts its use in signature creation to its signatory. The digital signature created with the TOE is a *qualified electronic signature* as defined in **The Directive** if the certificate for the SVD is a qualified certificate (Annex I). Determining the state of the certificate as qualified in beyond the scope of this standard.

The signature creation application shall 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 values 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 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. If the signature-creation application handles requesting obtaining a VAD from the user, it shall protect the confidentiality of this data.

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 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.

5.4.2 Target of Evaluation

The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory.

The TOE provides the following functions:

- to generate signature-creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification,
- to, optionally, receive and store certificate info,
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
  - (a) select an SCD if multiple are present in the SSCD,
  - (b) receive data to be signed or a unique representation thereof (DTBS/R)
  - (c) authenticate the signatory and determine its intent to sign,
  - (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 also conform to the specifications in ETSI TS 101 733 (CAdES)[6] and ETSI TS 101 903 (XAdES)[7]. In this case the TOE may provide additional supporting functions, e.g. to support receiving and/or validating a time stamp.

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

The TOE is prepared for the signatory's use by

- generating at least one SCD/SVD pair, and
- 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 preparation the SCD shall be 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, providing this information shall protect the confidentiality of the corresponding RAD.

If continued use of an SCD is no longer required the TOE will disable an SCD it holds, e.g. by erasing it from memory.

5.4.3 TOE life cycle

5.4.3.1 General

The TOE life cycle in figure 2 distinguishes stages for development production, preparation and operational use. The development and production of the TOE (cf. CC part 1, para.139) together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE to an SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to an SSCD-provisioning service provider.

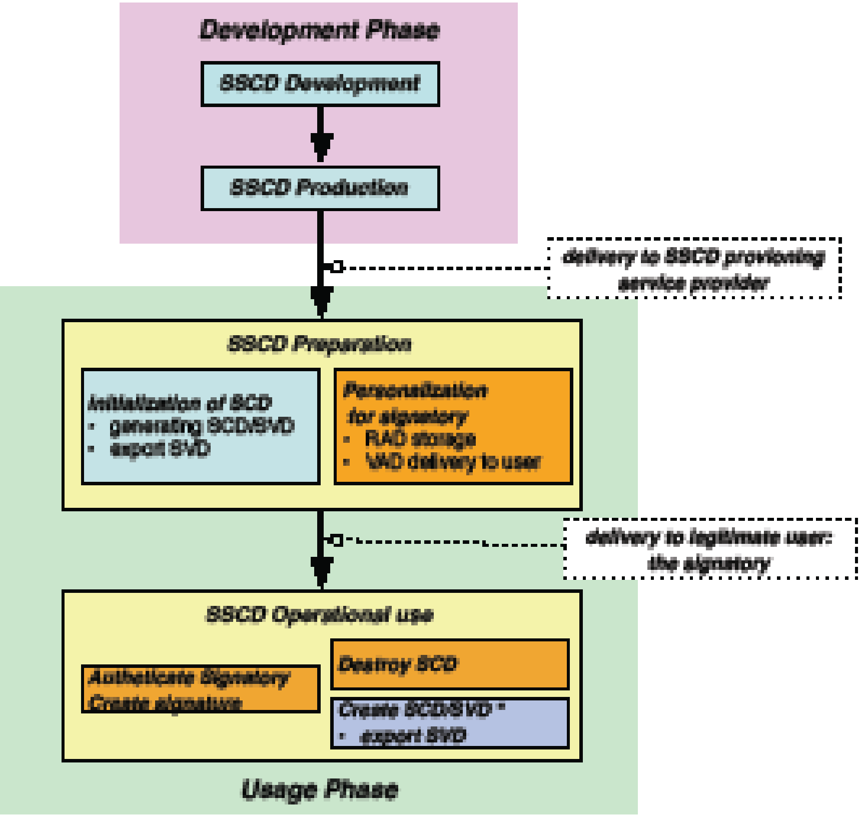

Figure 2: TOE life cycle

The TOE operational use stage begins when the signatory performs the TOE operation to enable it for use in signing operations. Enabling the TOE for signing requires at least one key stored in its memory. The TOE life cycle ends when all keys stored in it have been rendered permanently unusable. Rendering a key in the SSCD unusable may include deletion of the any stored corresponding certificate info.

5.4.3.2 Preparation stage

An SSCD-provisioning service provider having accepted it from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The preparation phase ends when the legitimate user of the TOE, having received it from an SSCD provisioning service enables if an SCD it holds for use in signing. During preparation of the TOE, as specified above, an SSCD-provisioning service provider performs the following tasks:

- Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.
- Generate a PIN and/or obtain a biometric sample of the legitimate user, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.
- Generate a certificate for at least one SCD either by:

   a. The TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or
   b. Initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE,
- Optionally, present certificate info to the SSCD.
- Deliver the TOE and the accompanying VAD info to the legitimate user.

The SVD certification task (third list item above) of an SSCD-provisioning service provider as specified in this PP may support a centralised, pre-issuing key generation process, with at least one key generated and certified, before delivery to the legitimate user. Alternatively, or additionally, that task may support key generation by the signatory after delivery and outside the secure preparation environment. A TOE may support both key generation processes, for example with a first key generated centrally and additional keys generated by the signatory in the operational use stage.

Data required for inclusion in the SVD certificate at least includes (**Annex** II):
- The SVD;
- The name of the signatory either
  (a) A legal name, or
  (b) A pseudonym together with an indication of this fact.

The data included in the certificate may have been stored in the SSCD during personalization.

Before initiating the actual certificate signature the certificate-generating application verifies the SVD received from the TOE by:
- establishing the sender as genuine SSCD
- establishing the integrity of the SVD to be certified as sent by the originating SSCD,
- establishing that the originating SSCD has been personalized for the legitimate user,
- establishing correspondence between SCD and SVD, and
- an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Optionally, the TOE may support a function to provide an explicit proof of correspondence between an SCD it stores and an SVD realized by self-certification. Such a function may be performed implicitly in the SVD export function and may be invoked in the preparation environment without explicit consent of the signatory[6]. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in a separate PP (see section 5.3).

Prior to generating the certificate the certification service provider shall assert the identity of the signatory specified in the certification request as the legitimate user of the TOE.

5.4.3.3 Operational use stage

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

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.

[6] Self-certification of the SVD is effectively computing a digital signature with the corresponding SCD. A signing operation requires explicit sole signatory control, this specific case, if supported, provides an exception to this rule as, before being delivered to the signatory, such control is evidently impossible.

The TOE may support functions to generate additional signing keys. If the TOE supports these functions it shall 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[7]. 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.

6 Conformance Claims

6.1 CC Conformance Claim

This Protection Profile is conforming to the Common Criteria version 3.1 Revision 3 [2] [3] [4].

This PP is conforming to Common Criteria Part 2 [3] extended and to Common Criteria Part 3 [4].

6.2 PP Claim, Package Claim

This Protection Profile 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].

6.3 Conformance rationale

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

6.4 Conformance Statement

The Protection Profile requires **strict** conformance of the ST or PP claiming conformance to this PP.

[7] 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.

7 Security Problem Definition

7.1 General

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

Assets and objects:

1. SCD: private key used to perform a digital 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 digital 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 digital signature must be maintained.

4. Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.

User and subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. In the TOE 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. In the TOE the subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.

3. Signatory: User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

1. Attacker as being a human or process acting on his behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the digital signature. An attacker has a high attack potential and knows no secret.

7.2 Threats

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 T.SVD_Forgery Forgery of the signature-verification data

An attacker presents a forged SVD to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

7.2.5 T.SigF_Misuse Misuse of the signature-creation function of the TOE

An attacker misuses the signature-creation function of the TOE to create a digital signature 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.

7.2.6 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.

7.2.7 T.Sig_Forgery Forgery of the digital signature

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. The signature generated 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.

7.3 Organisational Security Policies

7.3.1 P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (**The Directive**: 2:9, **Annex** I) for the SVD generated by the SSCD. 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.

7.3.2 P.QSign *Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with an advanced electronic signature (**The Directive**: 1, 2), which is a qualified electronic signature if it is based on a valid qualified certificate (**Annex** I)[8]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

7.3.3 P.Sigy_SSCD *TOE as secure signature-creation device*

The TOE meets the requirements for an SSCD laid down in **Annex** III This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

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

The life cycle 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 his un-revoked certificate.

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

7.4 Assumptions

7.4.1 A.CGA *Trustworthy certification-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.

7.4.2 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.

8 Security Objectives

8.1 General

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

8.2 Security Objectives for the TOE

8.2.1 OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD.

Application note 1: The TOE may contain more than one SCD. There is no need to destroy the SCD in case of re-generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after expiration of the (qualified) certificate for the corresponding SVD.

8.2.2 OT.SCD/SVD_Gen *SCD/SVD generation*

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

8.2.3 OT.SCD_Unique *Uniqueness of the signature-creation data*

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

8.2.4 OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

8.2.5 OT.SCD_Secrecy *Secrecy of the signature-creation data*

The secrecy of an SCD (used for signature creation) is 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/SVD generation, SCD signing operation, storage and by destruction.

8.2.6 OT.Sig_Secure *Cryptographic security of the digital signature*

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

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

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

8.2.8 OT.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

The TOE must not alter the DTBS/R This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

8.2.9 OT.EMSEC_Design *Provide physical-emanation security*

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

8.2.10 OT.Tamper_ID *Tamper detection*

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

8.2.11 OT.Tamper_Resistance *Tamper resistance*

The TOE prevents or resists physical tampering with specified system devices and components.

8.3 Security Objectives for the Operational Environment

8.3.1 OE.SVD_Auth *Authenticity of the SVD*

The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

8.3.2 OE.CGA_QCert *Generation of qualified certificates*

The CGA generates a qualified certificate that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP.

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

8.3.3 OE.SSCD_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalises and delivers the *TOE* as SSCD to the signatory.

8.3.4 OE.HID_VAD *Protection of the VAD*

If an external device provides the human interface for user authentication, this device will 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.

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

The Signatory uses trustworthy SCA that

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

8.3.6 OE.DTBS_Protect *SCA protects the data intended to be signed*

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

8.3.7 OE.Signatory *Security obligation of the Signatory*

The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The Signatory keeps his or her SVAD confidential.

8.4 Security Objectives Rationale

8.4.1 Security Objectives Coverage

Table 6.1-: Security problem definition to security objectives mapping

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	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													
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						
P.QSign						X	X					X				X		
P.Sigy_SSCD	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
A.CGA												X	X					
A.SCA																X		

8.4.2 Security Objectives Sufficiency

8.4.2.1 Policies and Security Objective Sufficiency

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

- the TOE security objective **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- the TOE security objective **OT.SCD_SVD_Corresp**, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and
- the security objective for the operational environment **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 generation function for the legitimate signatory only and to protect the SCD against the use of others. **OT.Sig_Secure** ensures that the TOE generates digital signatures that 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. The **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 **Annex** III. This is ensured as follows:

- **OT.SCD_Unique** meets the paragraph 1(a) of **Annex** III, by the requirements that the SCD used for signature generation can practically occur only once;
- **OT.SCD_Unique**, **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(a) of **Annex** III by the requirements to ensure secrecy of the SCD. **OT.EMSEC_Design** and **OT.Tamper_Resistance** address specific objectives to ensure secrecy of the SCD against specific attacks;
- **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(b) of **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** meets the requirement in paragraph 1(c) of **Annex** III by the requirements to ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE** meets the requirements in paragraph 2 of **Annex** III as the TOE must not alter the DTBS/R.

Paragraph 2 of **Annex** III, requires that an 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 it to the SSCD for signing.

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

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorised users only,
- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation 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 a TOE sample as an authentic, initialised and personalised SSCD from an 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 his 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 ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. **OE.SSCD_Prov_Service** ensures that the signatory uses an authentic TOE, initialised and personalised for the signator*y*. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once.

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. As prerequisite **OE.Signatory** ensures that the Signatory keeps his or her SVAD confidential. **OE.DTBS_Intend**, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may generate a valid digital 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.

8.4.2.2 Threats and Security Objective Sufficiency

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 recital (18) of **The Directive**. This threat is countered by **OT.SCD_Secrecy**, which assures the secrecy of the SCD used for signature creation.

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. **OT.SCD/SVD_Gen** counters this threat by implementing cryptographic secure generation of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure digital 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 exported by the TOE to the CGA to generation a certificate. T.SVD_Forgery is addressed by **OT.SCD_SVD_Corresp**, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and **OE.SVD_Auth** that ensures the integrity of the SVD exported by the TOE to the CGA.

T.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 a digital signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of **Annex** III. **OT.Lifecycle_Security** (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature-generation 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 a human interface for 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 that the Signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the Signatory becomes control over the SSCD. **OE.Signatory** ensures also that the Signatory keeps his or her SVAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS/R***)** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of **OE.DTBS_Intend**, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of **OE.DTBS_Protect**, which ensures that the DTBS/R can not 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 digital signature***)** deals with non-detectable forgery of the digital signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_Qcert** address this threat in general. The **OT.Sig_Secure**

(*Cryptographic security of the digital signature*) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. **OT.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 on a forged signature.

8.4.2.3 Assumptions and Security Objective Sufficiency

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 for the data that has 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 certification-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** (*Authenticity of the SVD*), which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

9 Extended Component Definition

The additional family FPT_EMSEC (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_EMSEC 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. The definition of the family FPT_EMSEC is taken from the *Protection Profile Secure Signature Creation Device* [5], chapter 6.6.1

FPT_EMSEC TOE Emanation

Family behaviour:
This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE Emanation
1

FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1
There are no management activities foreseen.

Audit: FPT_EMSEC.1
There are no actions identified that must be auditable if **FAU_GEN** (*Security audit data generation*) is included in a protection profile or security target.

9.1 FPT_EMSEC.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.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_EMSEC.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*].

10 IT Security Requirements

10.1 General

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Section 9 describes the extended component FPT_EMSEC.1. Section 10.2 provides the security functional requirements. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP into a Security Target (ST).

The TOE security assurance requirements statement is given in section 10.3.

10.2 TOE Security Functional Requirements

10.2.1 Use of requirement specifications

Common Criteria allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of part 2 of the CC. Each of these operations is used in this PP.

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is either (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.

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. A selection that has been made in this European standard is indicated as <u>underlined</u> text and the original text of the component is given by a footnote. Selections left 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. An assignment that that has been made in this European standard is indicated as <u>underlined</u> text and the original text of the component is given by a footnote. Assignments left 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.

10.2.2 Cryptographic support (FCS)

Application note 3: Member states of the European Union have specified entities as responsible for accreditation and supervision of the evaluation process for products conforming to this standard and for determining admissible algorithms and algorithm parameters (**The Directive**: 1.1b and 3.4). The ST writer shall consult with these entities to learn of admissible algorithms and cryptographic key sizes and other parameters or applicable standards.

10.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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

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

Application note 4: The ST writer shall perform the missing operations in the element FCS_CKM.1.1. The refinement in the element FCS_CKM.1.1 substitutes “cryptographic keys” by “SCD/SVD pairs” because it clearly addresses the SCD/SVD key generation.

10.2.2.2 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 5: The ST writer shall perform the missing operations in the element FCS_CKM.4.1. The specified cryptographic key destruction methods include but are not limited to overwriting the cryptographic key with any fixed or random data e.g. by generation of a new key.

10.2.2.3 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-generation[9] 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 6: The ST writer shall perform the missing operations in the element FCS_COP.1.1. The operations in the element FCS_COP.1.1 shall be appropriate for the SCD/SVD pairs generated according to FCS_CKM.1. Note that for some cryptographic algorithm like RSA padding is important part of the signature-generating algorithm.

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

10.2.3 User data protection (FDP)

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

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin - S.User acts as S.Admin R.Sigy - S.User acts as S.Sigy
S.User	SCD / SVD Management	Authorised, not authorised
SCD	SCD Operational	No, yes
SCD	SCD identifier	arbitrary value
SVD	(This PP does not define security attributes for SVD)	(This PP does not define security attributes for SVD)

Application note 7: The writer of PP or ST may define additional objects and security attributes.

10.2.3.1 FDP_ACC.1/SCD/SVD_Generation_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD/SVD_Generation_SFP The TSF shall enforce the SCD/SVD_Generation_SFP[10] on

(1) subjects: S.User,
(2) objects: SCD, SVD,
(3) operations: generation of SCD/SVD pair[11].

10.2.3.2 FDP_ACF.1/SCD/SVD_Generation_SFP *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/SVD_Generation_SFP The TSF shall enforce the SCD/SVD_Generation_SFP[12] to objects based on the following: the user S.User is associated with the security attribute "SCD / SVD Management "[13].

FDP_ACF.1.2/ SCD/SVD_Generation_SFP 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 generate SCD/SVD pair[14].

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

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

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

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

FDP_ACF.1.3/
SCD/SVD_Generation_SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[15].

FDP_ACF.1.4/
SCD/SVD_Generation_SFP

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 generate SCD/SVD pair[16].

10.2.3.3 FDP_ACC.1/SVD_Transfer_SFP *Subset access control*

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

FDP_ACC.1.1/
SVD_Transfer_SFP

The TSF shall enforce the SVD_Transfer_SFP[17] on

(1) subjects: S.User,

(2) objects: SVD

(3) operations: export[18].

10.2.3.4 FDP_ACF.1/SVD_Transfer_SFP *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/
SVD_Transfer_SFP

The TSF shall enforce the SVD_Transfer_SFP[19] to objects based on the following:

(1) the S.User is associated with the security attribute Role,

(2) the SVD [20].

FDP_ACF.1.2/
SVD_Transfer_SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [selection: *R.Admin, R.Sigy*] is allowed to export SVD[21].

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

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

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

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

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

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

[20] [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*]

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

FDP_ACF.1.3/ SVD_Transfer_SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[22].

FDP_ACF.1.4/ SVD_Transfer_SFP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[23].

Application note 8: The ST writer shall perform the operation in the element FDP_ACF.1.1/SVD_Transfer_SFP according to the access control rules provided by the TOE for SVD export. The access control rules may depend on TOE life cycle as shown in the following examples:

- The Administrator is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation_SFP and to export the SVD before the Signatory role (RAD) is created. This allows identification of a particular instance of the TOE by means of the SVD;
- The Administrator is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation_SFP and only the Signatory is allowed to export the SVD to the CGA. This allows determination whether the Signatory has control over the TOE instantiation and the certificate may be generated;
- The Signatory is authorized to generate the SCD/SVD key pair according to FDP_ACF.1/SCD/SVD_Generation_SFP and to export the SVD to the CGA to apply for the certificate.

This PP does not require the TOE to protect the integrity and authenticity of the exported SVD public key but requires such protection by the operational environment. If the operational environment does not provide sufficient security measures for the CGA to ensure the authenticity of the public key the TOE shall implement additional security functions to support the export of public keys with integrity and data origin authentication. See EN14169-3 “*Protection Profiles for Secure signature creation device - Part 3: Device with key generation and trusted channel between SSCD and CGA*” for additional requirements for use of an SSCD in an environment that cannot provide such protection.

10.2.3.5 FDP_ACC.1/Signature-creation_SFP *Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature-creation_SFP The TSF shall enforce the Signature-creation_SFP[24] on

(1) subjects: S.User,
(2) objects: DTBS/R, SCD,
(3) operations: signature-creation[25].

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

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

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

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

10.2.3.6 FDP_ACF.1/Signature-creation_SFP *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_SFP The TSF shall enforce the Signature-creation_SFP[26] to objects based on the following:

(1) the user S.User is associated with the security attribute “Role” and
(2) the SCD with the security attribute “SCD Operational”[27].

FDP_ACF.1.2/Signature-creation_SFP 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 digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”[28].

FDP_ACF.1.3/Signature-creation_SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[29].

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

S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “no”[30].

10.2.3.7 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[31] the following objects: SCD[32].

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

1. SCD
2. SVD (if persistently stored by the TOE).

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

[27] [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*]

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

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

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

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

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

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

10.2.3.8 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[33] on all objects, based on the following attributes: integrity checked stored data[34].

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[35].

10.2.3.9 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[36] on all objects, based on the following attributes: integrity checked stored DTBS[37].

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[38].

Application note 9: 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).

10.2.4 Identification and authentication (FIA)

10.2.4.1 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,

(2) [assignment: *list of additional TSF-mediated actions*][39]

on behalf of the user to be performed before the user is identified.

[33] [assignment: *integrity errors*]

[34] [assignment: *user data attributes*]

[35] [assignment: *action to be taken*]

[36] [assignment: *integrity errors*]

[37] [assignment: *user data attributes*]

[38] [assignment: *action to be taken*]

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

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 10: 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 life cycle, 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.

10.2.4.2 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*][40]

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 11: 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.

10.2.4.3 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[41].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[42], the TSF shall block RAD[43].

Application note 12: 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.

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

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

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

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

10.2.5 Security management (FMT)

10.2.5.1 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[44].

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

10.2.5.2 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) Change the default value of the security attribute SCD Identifier,
(5) [assignment: *list of other security management functions to be provided by the TSF*][45].

Application note 13: 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").

10.2.5.3 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[46] the functions signature-creation function[47] to R.Sigy[48].

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

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

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

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

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

10.2.5.4 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/SVD_Generation_SFP[49] to restrict the ability to modify [assignment*: other operations*][50] the security attributes SCD / SVD management[51] to R.Admin[52].

10.2.4.5 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[53] to restrict the ability to modify[54] the security attributes SCD operational[55] to R.Sigy[56].

10.2.5.6 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[57].

Application note 14: The ST writer shall define which values of the security attribute SCD / SVD Management are secure for the TOE and the intended TOE life cycle. E.g. if the TOE supports generation of

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

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

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

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

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

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

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

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

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

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”.

10.2.5.7 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/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-creation_SFP[58] to provide restrictive[59] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the R.Admin[60] to specify alternative initial values to override the default values when an object or information is created.

10.2.5.8 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 successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation.

(2) If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation. [61]

Application note 15: The TOE may not support generating an SVD/SCD pair by the Signatory alone, in which case rule (2) is not relevant.

10.2.5.9 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[62] the RAD[63] to R.Admin[64].

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

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

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

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

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

10.2.5.10 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*] [65] the RAD[66] to R.Sigy[67].

Application note 16: The ST writer shall perform the missing operation in the element FMT_MTD.1.1. The missing assignment may be “unblock” or “none”.

10.2.6 Protection of the TSF (FPT)

10.2.6.1 FPT_EMSEC.1 *TOE Emanation*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit [assignment*: types of emissions*] in excess of [assignment*: specified limits*] enabling access to RAD[68] and SCD[69].

FPT_EMSEC.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[70] and SCD[71].

Application note 17: 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.

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

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

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

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

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

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

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

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

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

10.2.6.2 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*][72].

Application note 18: 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.

10.2.6.3 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.

10.2.6.4 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 19: 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 a failure of TOE start-up as indication of physical tampering.

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

10.2.6.5 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[73].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[74].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of TSF[75].

Application note 20: 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. 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.

10.3 TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL4 augmented with AVA_VAN.5

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

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

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

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

Assurance Class	Assurance components
	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

11 Rationale

11.1 Security Requirements Rationale

11.1.1 Security Requirement Coverage

Table 6.2 : Functional Requirement to TOE security objective mapping

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	X		X	X	X						
FCS_CKM.4	X				X						
FCS_COP.1	X					X					
FDP_ACC.1/ SCD/SVD_Generation_SFP	X	X									
FDP_ACC.1/ SVD_Transfer_SFP	X										
FDP_ACC.1/Signature-creation_SFP	X						X				
FDP_AFC.1/ SCD/SVD_Generation_SFP	X	X									
FDP_AFC.1/ SVD_Transfer_SFP	X										
FDP_AFC.1/Signature-creation_SFP	X						X				
FDP_RIP.1					X		X				

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FDP_SDI.2/Persistent				X	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	X									
FMT_MSA.1/Signatory	X						X				
FMT_MSA.2	X	X					X				
FMT_MSA.3	X	X					X				
FMT_MSA.4	X	X					X				
FMT_MTD.1/Admin	X						X				
FMT_MTD.1/Signatory	X						X				
FMT_SMR.1	X						X				
FMT_SMF.1	X						X				
FPT_EMSEC.1					X				X		
FPT_FLS.1					X						
FPT_PHP.1										X	
FPT_PHP.3					X						X
FPT_TST.1	X				X	X					

11.1.2 TOE Security Requirements Sufficiency

OT.Lifecycle_Security (*Lifecycle security*) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP. The SCD usage is ensured by access control FDP_ACC.1/Signature-creation_SFP, FDP_AFC.1/Signature-creation_SFP 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, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD/SVD_Gen (*SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR

FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (*Uniqueness of the signature-creation data*) implements the requirement of practically unique SCD as laid down in **Annex** III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SCD_SVD_Corresp (*Correspondence between SVD and SCD*) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (*Secrecy of signature-creation data*) is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. 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).

SFR FPT_EMSEC.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 digital signature*) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures 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 ensure self-tests ensuring correct signature-creation..

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

FIA_UAU.1 and FIA_UID.1 ensure that no signature generation 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. 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 and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).

The security functions specified by FDP_ACC.1/Signature-creation_SFP and FDP_ACF.1/Signature-creation_SFP provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. 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. FMT_MOF.1 restricts the ability to enable the signature-creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

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

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

11.2 Dependency Rationale for Security functional Requirements

The following table provides an overview how the dependencies of the security functional requirements are solved and a justification why some dependencies are not being satisfied.

Table 6.5 Functional Requirements Dependencies

Requirement	**Dependencies**	**Fulfilled**
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/ SCD/SVD_Generation _SFP	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP
FDP_ACC.1/ Signature-creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature-Creation SFP
FDP_ACC.1/ SVD_Transfer_SFP	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP
FDP_ACF.1/ SCD/SVD_Generation _SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation_SFP, FMT_MSA.3
FDP_ACF.1/ Signature-creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature-creation_SFP, FMT_MSA.3
FDP_ACF.1/ SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP, FMT_MSA.3
FDR_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_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
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/SVD_Generation_SFP, 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 SFP, FMT_SMR.1, FMT_SMF.1

Requirement	Dependencies	Fulfilled
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/Signature_Creation SFP, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
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/SVD_Generation_SFP, FDP_ACC.1/ Signature-creation_SFP
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_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.

11.3 Rationale for EAL 4 Augmented

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. The component AVA_VAN.5 has the following dependencies:

ADV_ARC.1 Architectural Design with domain separation and non-bypassability
ADV_FSP.4 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

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

12 Bibliography

[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-0006-2002T, also short SSVG-PPs or CWA14169

[6] ETSI Technical Specification 101 733: CMS Advanced Electronic Signatures (CAdES), V.1.7.4, 2008-07

[7] ETSI Technical Specification 101903: XML Advanced Electronic Signatures (XAdES), V.1.3.2, 2006-03