Security Target Lite STARCOS 3.4 Health AHC C1

Version 2.3/17.12.09

Author: Giesecke&Devrient GmbH
Document status: Final Version

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
81607 München

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Content

1 Introduction

1.1 TOE Reference

This document refers to the following TOE(s):

1) STARCOS 3.4 Health AHC C1

1.2 ST Reference and ST Identification

Title: Security Target Lite STARCOS 3.4 Health AHC C1

Version Number/Date: Version 2.3/17.12.09

Origin: Giesecke & Devrient GmbH

TOE: STARCOS 3.4 Health AHC C1

TOE documentation:

- Guidance Documentation STARCOS 3.4 Health AHC C1 - Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health AHC C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health AHC C1
- Guidance Documentation for the Usage Phase STARCOS 3.4 Health AHC C1
- Generic Application of STARCOS 3.4 Health AHC C1
- STARCOS 3.4 SmartCard Operating System Reference Manual
- Smart Card Application Verifier

HW-Part of TOE: NXP P5CC052V0A (Certificate: BSI-DSZ-CC-0466-2008)

1.3 TOE Overview

The aim of this document is to describe the Security Target for 'STARCOS 3.4 Health AHC C1'.

The related product is the STARCOS 3.4 Operating System (OS) on a Smart Card Integrated Circuit. It is intended to be used as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [1], so the TOE consists of the part of the implemented software related to the generation of qualified electronic signatures in combination with the underlying hardware ('Composite Evaluation'). The functional and assurance requirements for SSCDs defined in Annex III of this EU Directive [1] have been mapped into a Protection Profile (PP) for Secure Signature Creation Devices of Type 3 (onboard generation of the signature key). The 'Security

Target STARCOS 3.4 Health AHC C1' is compliant to the core PP for SSCDs of Type 3 (generation of SCD/SVD pair, storage of Signature Creation Data and Signature Creation Component) [5].

STARCOS 3.4 is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library enabling the user to generate high security electronic signatures based on ECDSA GF(p) with a key length of 256 bit. The EU compliant Electronic Signature Application is designed for the creation of legally binding Qualified Electronic Signatures as defined in the EU Directive [1]. The various features of STARCOS 3.4 allow for additional applications health system related applications.

The software part of the TOE is implemented on the certified NXP P5CC052V0A [8]. So the TOE consists of the software part and the underlying hardware. The RSA2048 crypto library provided with the underlying hardware is not used in this composite TOE. The software part of the calculations based on elliptic curves is implemented in the operating system. The corresponding Security Target (Lite) [9] is compliant to the BSI-PP-0002-2001 [10].

This document describes

- the Target of Evaluation (TOE)
- the security environment of the TOE
- the security objectives of the TOE and its environment
- and the TOE security functional and assurance requirements.

The assurance level for the TOE is CC **EAL4+**.

1.4 CC Conformance

This ST is in accordance with Common Criteria V3.1 (see [2], [3], [4]).

This ST is compliant with CC V3.1 Part 2 [3], extended by an additional functional component as stated in [5] and another additional functional component.

This ST is compliant with CC V3.1 Part 3 [4], level **EAL4** augmented by

- AVA_VAN.5

as stated in [5].

1.5 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the TOE description.

Section 3 contains the conformance claims.

Section 4 contains the Security Problem Definition

Section 5 defines the security objectives for both the TOE and the TOE environment. In addition, a rationale is provided to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 6 contains the Extended component definition.

Section 7 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied.

Section 8 contains the TOE Summary Specification.

Section 9 provides an explanation how the set of security requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 9 provides a set of arguments that address dependency analysis.

Section 10 provides definitions of frequently used acronyms.

Section 11 provides information on applied conventions and used terminology.

Section 12 provides a list of references used throughout the document.

2 TOE Description

2.1 Product Type

(The following description should be used as general introduction to SSCDs.)

2.1.1 Types of Secure Signature Creation Devices

The present document assumes a well-defined process of signature-creation to take place. The present subchapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1. The SSCD Type 1 generates pairs of corresponding SCD and SVD (SCD/SVD pairs) and exports SCD for the use in SSCD Type 2. The SSCD Type 2 imports SCD generated by SSCD Type 1 and creates signatures. The SSCD Type 3 generates SCD/SVD pairs and generates signatures with SCD. A SSCD may generate SCD/SVD pairs (as SSCD Type 3) and import SCD from a SSCD Type 1 (as SSCD Type 2). The SSCD Type 2 and SSCD Type 3 must not export the SCD. Only SSCD Type 2 and SSCD Type 3 create signatures with stored SCD for DTBS provided by the signature-creation application (SCA).

The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and an SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on an SSCD Type 1 shall be exported to an SSCD Type 2. The right part of Figure 1 shows an SSCD Type 3, which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided. The SSCD Type 2 and SSCD Type 3 have interfaces to the SCA for import of DTBS and export of signatures.

The certificate generation application (CGA) initiates SCD/SVD generation ("Initialisation") and the SSCD exports the SVD for generation of the corresponding certificate by the CGA of the certification-service-provider (CSP) ("SVD to CSP"). In case of SSCD Type 2 the SSCD Type 1 must protect the confidentiality of the SCD during the generation of the SCD/SVD pair and the export to the SSCD Type 2. If the SSCD holds the SVD and exports the SVD to a CGA for certification than the integrity of the SVD shall be protected by the SSCD or the environment.

SSCD Type 1 is not necessarily a personalized component in the sense that a specific user only may use it. But only authorized persons shall initiate the SCD/SVD generation and export (e.g., system administrator). SSCD Type 2 and Type 3 are personalized components, which means that only one specific user – the signatory - can use signature creation by the SSCD.

The signatory must be authenticated to create signatures. If the human interface (HI) to capture the VAD is not provided by the SSCD, the SCA shall provide the HI and protect

the confidentiality and integrity of the VAD as appropriate for the authentication method.

The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be protected in integrity while transferred by the SCA to the SSCD. This integrity protection may be provided by the SCA sending the DTBS and supported by the SSCD receiving the DTBS.

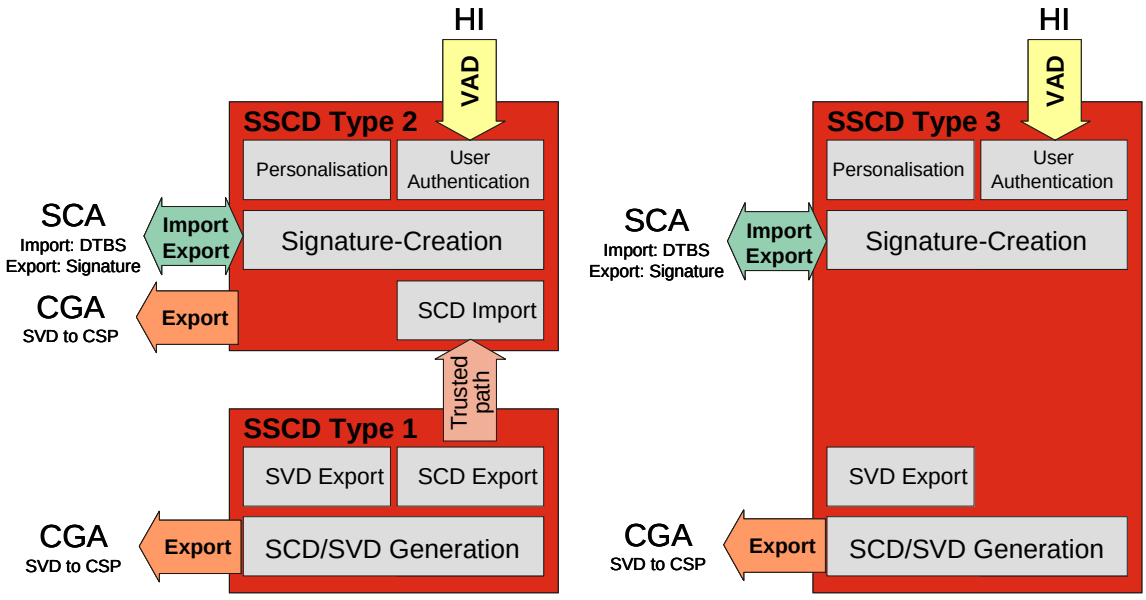


Figure 1: SSCD types and modes of operation

2.1.2 Target of Evaluation (TOE)

The TOE is a secure signature-creation device (Type 3) according to Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. An SSCD is configured software or hardware used to implement the signature-creation-data (SCD). The SSCD protects SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory.

The TOE provides the following functions necessary for devices involved in creating advanced electronic signatures[1]:

(1) to generate SCD and the correspondent signature-verification data (SVD),

(2) to export the SVD, and

(3) to create digital signatures for the data to be signed

(a) after appropriate authentication of the signatory by the TOE,

(b) applying appropriate cryptographic signature-creation function using the selected SCD to the data to be signed.

[1]The Directive [1], recital (15), refers to SSCDs according Annex III to ensure the functionality of advanced signatures.

The digital signature created with a SCD implemented in the SSCD can be used for qualified electronic signature if it is based on a valid qualified certificate (according to the Directive [1], Annex I).

The TOE comprises all IT security functionality, which is necessary to ensure the secrecy of the SCD and the security of the digital signature. The TOE is intended for usage by the signer in a secure operational environment. When a SCD/SVD pair is generated by a certification service provider this shall be done in a secure environment as well, so that the TOE can be delivered to the signer with at least one SCD / SVD pair stored in it.

The TOE will be prepared for the signatory's use by
(1) generating a SCD/SVD pair and
(2) personalisation for the signatory by means of the signatory’s verification authentication data (VAD).

The TOE will be prepared for the signatory's use by defining the value of the signatory’s reference authentication data (RAD). The legitimate user should be informed of the value of the signatory’s verification authentication data (VAD). The SCD is in non-operation state. The signatory shall verify this non-operational state at reception and change the SCD state to operational.

The TOE is intended for usage by the signer in a secure operational environment. When a SCD/SVD pair is generated by a certification service provider this shall be done in a secure environment as well, so that the TOE can be delivered to the signer with at least one SCD / SVD pair stored in it.

The TOE stores the SCD securely protecting its confidentiality and exports the SVD.

This ST requires that the SSCD ensures the integrity of the exported SVD during transmission to the certificate generation application (CGA) of the certification-service-provider (CSP). The underlying SSCD core PP [5] requires the operational environment to ensure authenticity of the SVD during transmission to the CGA of the CSP. So compared to the SSCD core PP this ST has been augmented with respect to this issue.

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory.

The signatory uses a signature-creation system (SCS) to create an electronic signature for data. The SCS consists of the signature-creation application (SCA) and the SSCD. The SCA prepares and presents the data to be signed (DTBS) to the signatory prior to the signature process and sends DTBS-representation to the SSCD. The signatory initiates the signature-creation by the SSCD for an unambiguously referenced SCD on the SSCD and the DTBS-representation is sent to the SSCD. The SSCD creates the digital signature by application of a cryptographic signature-creation function to the DTBS-representation provided by the SCA and using the SCD as parameter. The SCA generates an electronic signature by using the digital signature returned by the SSCD.

This ST requires the operational environment to ensure integrity of DTBS provided by the SCA to the TOE. This ST assumes the SCA as environment of the TOE because the ST describes the SCD-related security objectives and requirements, whereas the SCA does not implement the SCD.

Typical examples of the TOE are smart cards, which are used with smart card terminals for input of PIN as the user verification authentication data (VAD) and signature application running on personal computer.

The TOE provides user authentication and access control to prevent unauthorised generation of the SCD/SVD pair and usage of the SCD. The user may authenticate themselves to the TOE by knowledge of verification authentication data (VAD). The TOE holds reference authentication (RAD) and checks the provided VAD. The interface for authentication of technical components (e.g. a token used by the signatory) may be very simple while a human interface for authentication implies appropriate hardware. The authentication interface for human users like the signatory are implemented by an external human interface device (HID) connected with the SSCD or an external HID connected with the SCA, which communicates with the SSCD.

The ST assumes a secure external human interface device (typically as part of the SCA) for signatory's authentication and requires the environment to protect the confidentiality and integrity of the VAD as appropriate for the authentication method used by the TOE.

2.2 Limits of the TOE

(Some subchapters are according to the SSCD Protection Profile [5] with modifications where necessary.)

2.2.1 Intended use of the TOE

The TOE is implemented as a Smart Card on an IC and is intended to be used as Secure Signature Creation Device. This includes the Generation and Secure Storage of a SCD/SVD pair and the generation of Qualified Electronic Signatures using ECDSA GF(p) with a key length of 256 bit. Before the SCD/SVD pair is re-generated, the previous content is destroyed. Generation of the SCD is only possible for the administrator.

Beside this the use of multiple separated additional applications like health system related applications is possible. Therefore the TOE provides ISO 7816 compliant commands for the different kinds of applications. Due to security reasons the commands provided by the TOE cannot be altered or extended after delivery, therefore all applications can only be realised with the existing commands.

2.2.2 Structural view of the TOE

The TOE is a secure signature-creation device (SSCD Type3) according to Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1].

The TOE is realised by a smartcard, consisting of the embedded software residing on the underlying certified IC. The TOE comprises the certified chip, the operating system STARCOS 3.4, the documentation (Guidance Documentation of STARCOS 3.4 Health AHC C1, Generic Application Specification of STARCOS 3.4 Health AHC C1, Smart Card Application Verifier[2]). The operating system STARCOS 3.4 is implemented in the ROM area of the IC, whereas some parts may also reside in the EEPROM. The file system containing the application data is installed in the EEPROM of the IC. Beside the files for the digital signature application there may be additional files for other applications, e.g. for the health system, which do not belong to the TOE. The file system part of the TOE is represented by the Guidance Documentation and the Generic Application Specification that define the security relevant parts of the file system. The Smart Card Application Verifier verifies the correctness of the file system after installation of the TOE.

[2] The Smart Card Application Verifier and the corresponding representation of Generic Signature Application STARCOS 3.4 Health AHC C1 are not part of the TOE delivery. They are solely used by G&D to verify that the signature application conforms to the requirements of the Generic Signature Application STARCOS 3.4 Health AHC C1.

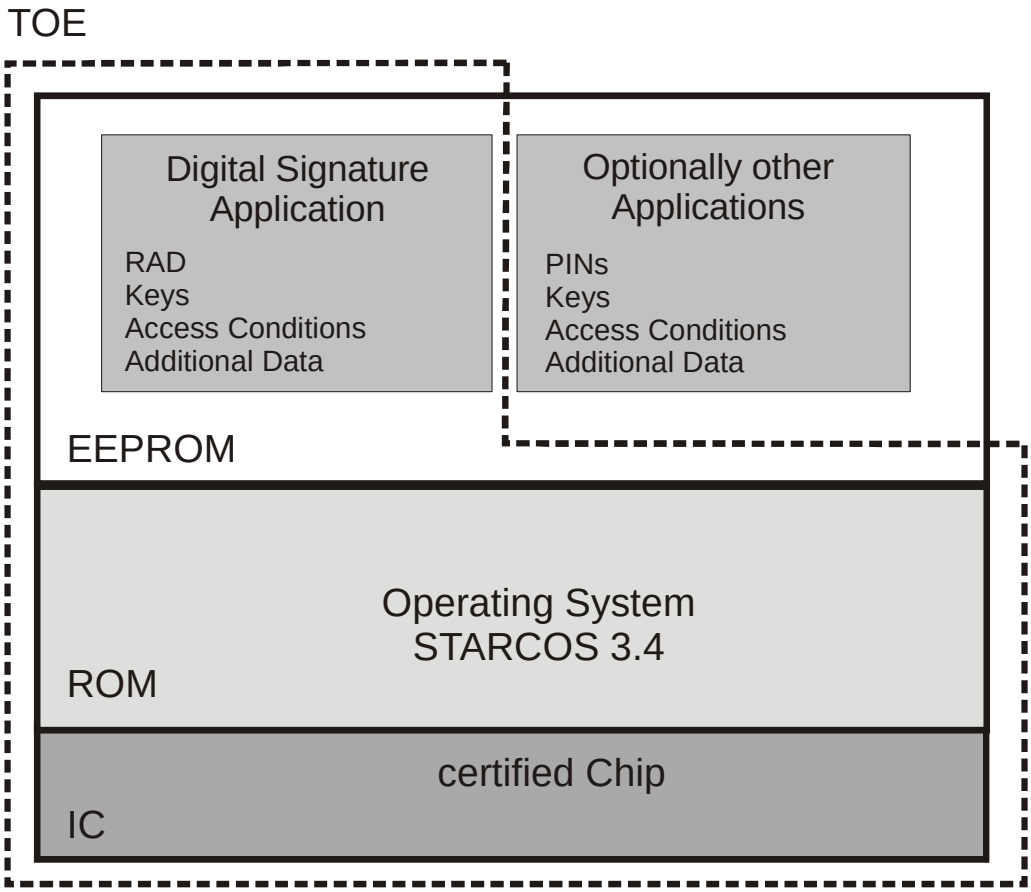


Figure 2: TOE description (after installation)

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

(a) after allowing for the data to be signed (DTBS) to be displayed correctly by an appropriate environment

(b) using appropriate hash functions that are, according to [6], agreed as suitable for qualified electronic signatures

(c) after appropriate authentication of the signatory by the TOE

(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [6].

The TOE ensures for the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The user authenticates himself with the knowledge of the Verification Authentication Data (VAD) against the Reference Authentication Data (RAD) securely stored inside the card.

The TOE does not implement the signature-creation application (SCA), that presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. So this ST assumes the SCA as environment of the TOE.

The TOE protects the SCD during the whole life cycle as to be solely used in the signature creation process by the legitimate signatory. The SSCD of Type 3 generates the signatory's SCD and stores it in a secure manner. The TOE will be personalised for the signatory's use by

(1) generation of the SCD/SVD pair,

(2) personalisation for the signatory by means of the signatory’s verification authentication data (VAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP).

From the structural perspective, the SSCD (which is represented by the TOE after installation) comprises the underlying IC, the STARCOS 3.4 operating system (OS) and the signature application providing the functionality for SCD/SVD generation, authentic SVD export, SCD storage and use, and generation of electronic signatures. The SCA and the CGA (beside optional other applications) are part of the immediate environment of the TOE. The TOE implements IT measures to support the establishment of a trusted channel by cryptographic means to export the SVD to the Certification Generation Application (CGA). There is no cryptographic protection of the communication between SCA and the TOE, therefore the TOE shall only be used within a Trusted Environment to create electronic signatures.

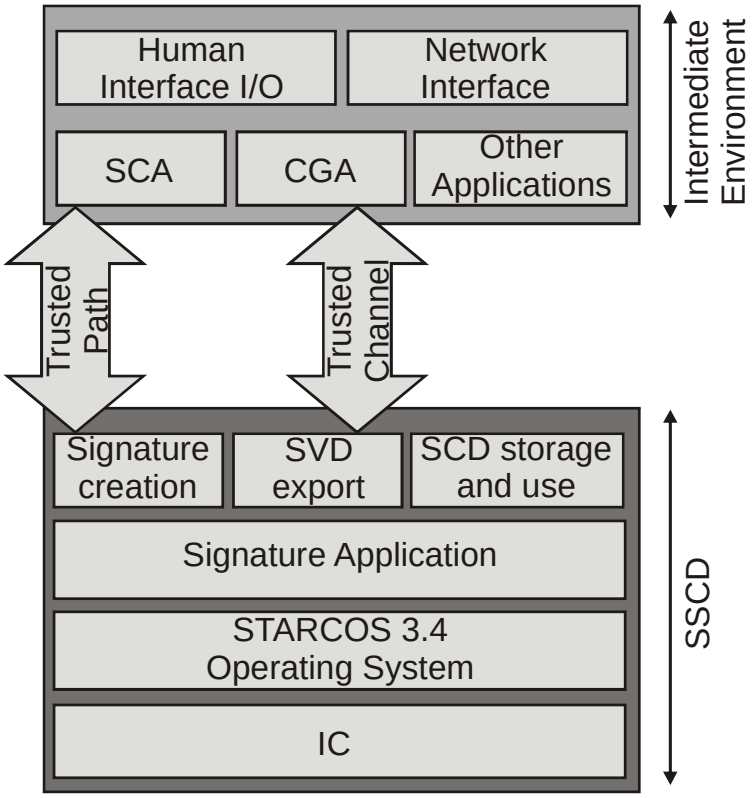


Figure 3: Scope of the SSCD, structural view

Beside the Signature Application there are also additional applications possible to reside on the card. These additional applications are using the same underlying IC and OS as the Signature Application. Each application, in particular the Signature Application, can define access rules to protect itself against misuse and unauthorised access. Usually the data structures for applications are loaded onto the card during initialisation and personalisation. Nevertheless it is still possible to add some data structures in the usage phase to the Signature Application like loading the qualified certificate for the SCD. Furthermore the complete data structures of additional applications may be loaded during the usage phase. These data structures does not include any executable code, therefore application functionality is always limited to the functionality of the operating system.

2.2.3 TOE life cycle

The TOE life cycle is shown in Figure 3. This life cycle only applies when the TOE is prepared in a secure environment and delivered to the signatory with one SCD. Basically, it consists of a Development Phase and the operational Usage Phase.

The Development Phase comprises the development and the production of the TOE (cf. CC part 1, para.139). The Development Phase is subject of the evaluation according to

the assurance life cycle (ALC) class. The Development Phase ends with the delivery of the TOE parts to the SSCD provision service.

The operational usage of the TOE comprises the preparation phase (i.e. initialisation and personalisation of the TOE) and the operation phase.

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

(1) The personalization of TOE for use signatory i.e. the installation of the RAD in the TOE and handover of VAD to the signatory.
(2) The initialization of the TOE i.e. generation of SCD/SVD pair by the TOE, storage of the SCD in the TOE and export of the SVD.
(3) The generation of the certificate containing among others (cf. [1], Annex II)
the SVD which correspond to SCD under the control of the signatory;
the name of the signatory or a pseudonym, which shall be identified as such.
(4) The preparation may include optional loading of Certificates or Certificate info into the SSCD for signatory convenience.
The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of

(a) the (internal) SSCD proof of correspondence between SCD and SVD,
(b) checking the sender and integrity of the received SVD,
(c) an SVD value originates from a given SSCD, and that
(d) the algorithm and key size for the SVD are appropriate.

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

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

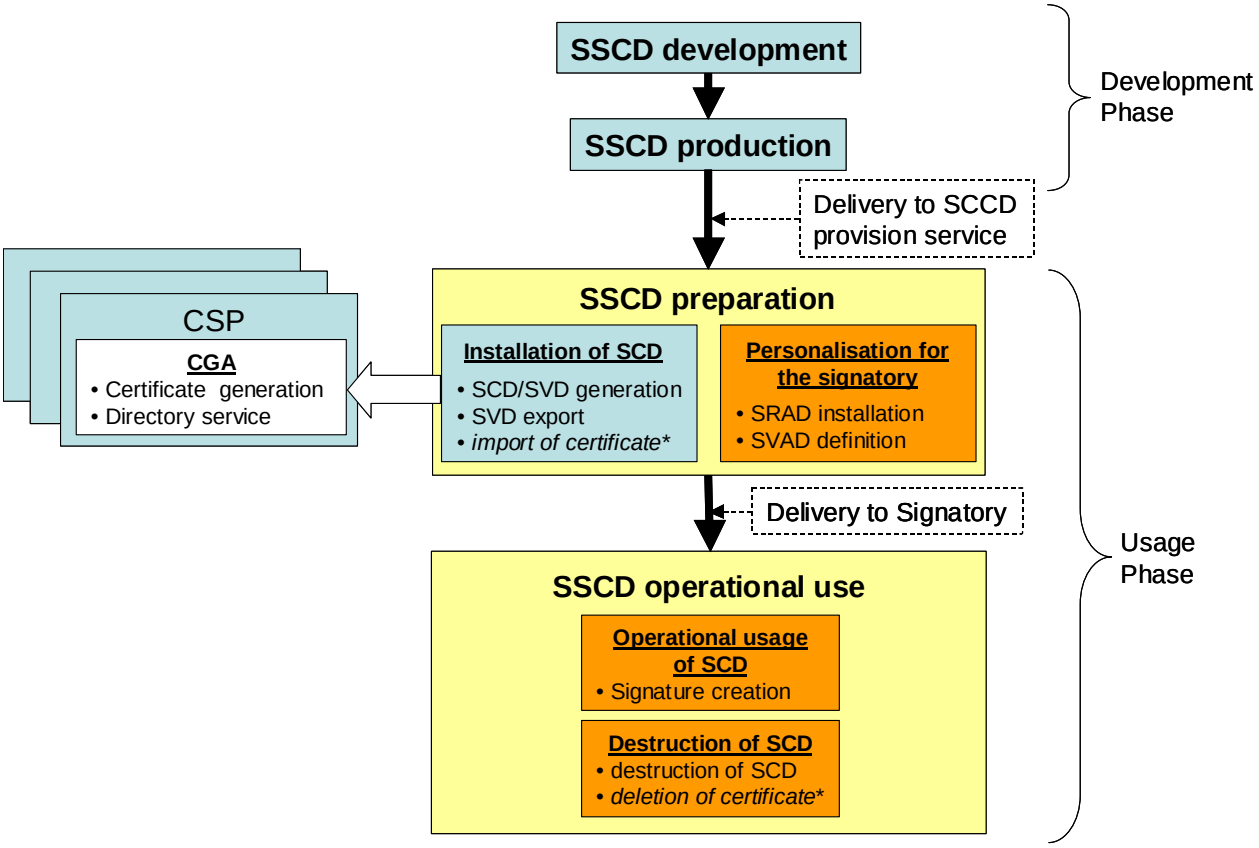


Figure 4: Typical TOE life cycle[3]

The CSP will generate a certificate only if the SCD is stored in a SSCD and if it has verified the credentials presented by the signatory. An uninterrupted secured TOE delivery chain from the manufacturer through the SSCD delivery service to the signatory assures this property.

This ST requires the TOE to provide mechanisms for generation of SCD/SVD pairs, implementation of the SCD and personalization. The environment shall protect all other processes for TOE preparation like SVD export to the CGA.

The operational phase of the TOE starts when the SCD / SVD pair is generated by the SSCD and when the signatory takes control over the TOE. The signatory uses the TOE with trustworthy SCA in secured environment only. The SCA shall protect the integrity of the DTBS during the transmission to the TOE.

The TOE life cycle as SSCD ends when the SCD implemented in the TOE is destructed. Remark: This might be done by physically destroying the smart card chip.

2.2.4 Delivery of ROM-Mask and initialisation data

As shown in Fig. 2, the Software part of the TOE consists of the STARCOS 3.4 operating system located in the ROM of the IC and the File System located in the

[3]The stars * mark the optional import of the certificate info and the deletion of the certificate info (which may include the certificate).

EEPROM. Parts of the operating system may also reside in the EEPROM. The operating system developer (i.e. G&D) creates the ROM mask and sends this representation of the operating system together with secret data allowing secure loading of initialisation data to the Chip Manufacturer (see Fig. 5). The Chip manufacturer manufactures the chips including the operating system and stores the secret data in a special area of the EEPROM of the Chip and delivers the chips packaged in modules to the Initialiser. The secret data is used by the OS developer to secure the initialisation data which is sent afterwards to the card initialising facility. The Card Initialising Facility manufactures the cards, performs the initialisation and then delivers the cards to the personalising facility.

With the secured initialisation data secret data is imported into the TOE allowing secure loading of personalisation data. This secret data is sent by the OS developer to the card issuer who uses it to secure the personalisation data and then send the secured personalisation data to the personalising facility which performs the personalisation before issuance of the TOE.

The Initialisation can be done completely by G&D. The Personalisation Process can be done partly or completely by G&D. The generation of the Personalisation data can also be done partly or completely at G&D.

During the personalisation before issuance, trust anchors can be imported into the TOE to allow a completion of the personalisation after issuance.

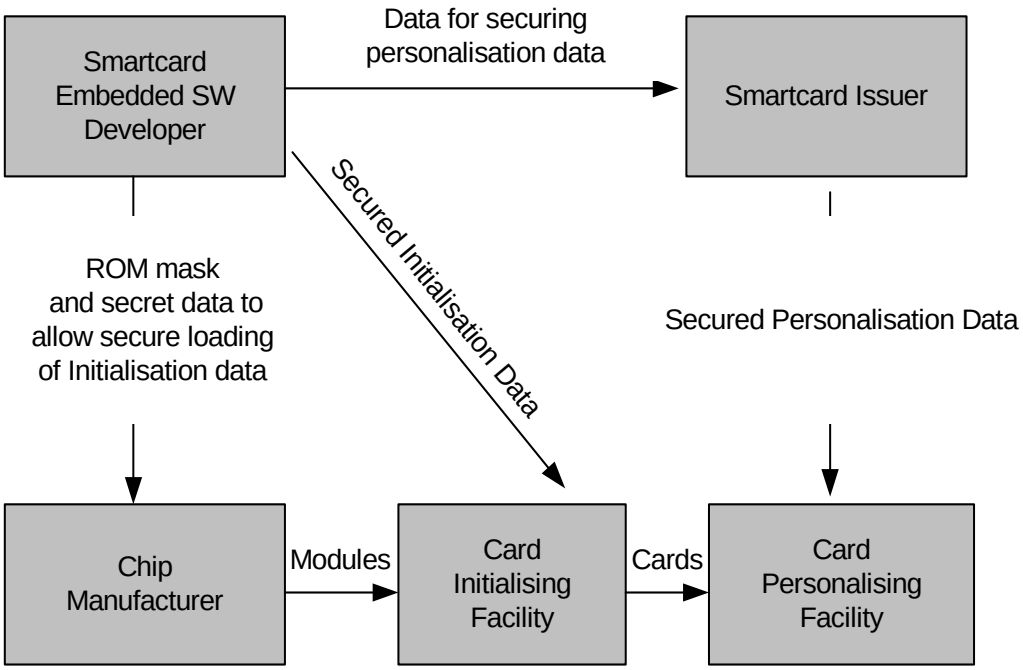


Figure 5: ROM Mask and initialisation data delivery

2.3 TOE operational environment

The TOE is used in two different types of operational environment. Prior to the issuance, the TOE has to be completed in the initialsation phase and the personalisation

phase. After the issuance, the signatory controls the TOE. In case the personalisation of the signature application was not finished before issuance, he can only use other applications existing on the card until he provides the TOE to a personaliser for finishing of the personalisation. The signatory mainly interacts with the personalised TOE via the SCA.

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target is Common Criteria version 3.1 Revision 3 [2] [3] [4] conformant.

This Security Target is Common Criteria Part 2 [3] extended and Common Criteria Part 3 [4] conformant.

3.2 PP Conformance Claim

This ST is based on the SSCD core PP Type 3 [5] as well as SSCD CGA PP [14] but is not formally compliant to any PP. Therefore no formal conformance to a PP is claimed.

3.3 Package Conformance Claim

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

3.4 Conformance Claim Rationale

This part is not applicable to this ST.

4 Security Problem Definition

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:

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.

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.

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.

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

User and subjects acting for users:

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.

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.

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:

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

4.1 Threats

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.

T.SCD_Derive *Derive the signature-creation data*

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

T.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.

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.

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.

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.

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.

4.2 Organisational Security Policies

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. Directive [1], article 2, clause 9, and 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.

P.QSign *Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with an advanced electronic signature (cf. Directive, Article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the Directive Annex I)[4]. 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.

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

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

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

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.

4.3 Assumptions

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 signature of the CSP.

A.SCA *Trustworthy signature-creation application*

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

5 Security Objectives

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.

5.1 Security Objectives for the TOE

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.

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.

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.

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 signature creation with the SCD.

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

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

Application note: The TOE shall keep the confidentiality of the SCD at all time in particular during SCD/SVD generation, SCD signing operation, storage and by destruction.

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.

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.

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.

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.

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.

OT.Tamper_Resistance *Tamper resistance*

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

OT.TOE_SSCD *Authentication proof as SSCD*

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate themselves as SSCD.

OT.TOE_TC_SVD_Exp *TOE trusted channel for SVD export*

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

5.2 Security Objectives for the Operational Environment

OE.SVD_Auth *Authenticity of the SVD*

The operational environment ensures the integrity of the SVD exported by the TOE to the CGA.

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.

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.

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.

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.

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 VAD confidential.

OE.CGA_SSCD *Pre-initialisation of the TOE as SSCD*

The CSP shall check by means of the CGA whether the device presented by the applicant for the (qualified) certificate examples holds unique identification as SSCD and is able to prove this identity.

OE.CGA_TC_SVD CGA *trusted channel for SVD*

The CGA shall detect alteration of the SVD imported from the TOE. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the (qualified) certificate.

5.3 Security Objectives Rationale

5.3.1 Security Objectives Coverage

The following table shows how the security objectives for the TOE and the security objectives for the environment cover the threats, organizational security policies and assumptions.

	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	OT.TOE_SSCD	OT.TOE_TC_SVD_EXP	OE.CGA_SSCD	OE.CGA_TC_SVD	OE.CGA_QCert	OE.SVD_Auth	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		X					
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X	X	X	X	X						
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X
A.CGA															X	X	X				
A.SCA																			X		

Table 1: Security problem definition to security objectives mapping

Augmentation

The following changes have been performed compared to the rationale in the SSCD core PP [5]:

- T.SVD_Forgery: OT.SCD_SVD_Corresp and OE.SVD_Auth have been replaced by OT.TOE_TC_SVD_EXP and OE.CGA_TC_SVD.
- P.QSign: OT.TOE_SSCD and OE.CGA_SSCD have been added; instead of mapping P.QSign to OT.Sig_Secure, OT.Sigy_SigF, OE.CGA_QCert and OE.DTBS_Intend, P.QSign is mapped to OT.Lifecycle_Security,

OT.SCD_SVD_Corresp, OT.TOE_SSCD, OE.CGA_QCert and OE.CGA_SSCD.

- P.Sigy_SSCD: OE.SSCD_Prov_Service has been replaced by OT.TOE_TC_SVD_EXP, OT.TOE_SSCD, OE.CGA_TC_SVD and OE.CGA_SSCD.
- P.Sig_Non-Repud: OE.SSCD_Prov_Service has been replaced by OT.TOE_TC_SVD_EXP, OT.TOE_SSCD, OE.CGA_TC_SVD and OE.CGA_SSCD.
- A.CGA: Assignment to OE.SVD_Auth_CGA (which hasn't been defined in the PP) has been replaced by OE.SVD_Auth. OE.CGA_TC_SVD has been added to the rationale. Verification of correspondence between SCD and SVD has been deleted, because this is covered by OT.SCD_SVD_Corresp.

5.3.2 Security Objectives Sufficiency

5.3.2.1 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, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The OE.CGA_QCert addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates. According OT.TOE_SSCD the TOE examples will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD based on theses pre-initialisation to prove this identity as SSCD to the CGA. The OE.CGA_SSCD ensures that the SP

checks the proof of the device presented of the applicant that it is a SSCD. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory. The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialisation, personalisation and operational usage.

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

- OT.SCD_Unique meets the paragraph 1(a) of the Directive [1], 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 the Directive [1], 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 the Directive [1], Annex III, by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of the Directive [1], 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 the Directive [1], Annex III, as the TOE must not alter the DTBS/R.

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

The objectives OT.TOE_SSCD, OT.TOE_TC_SVD_Exp, OE.CGA_SSCD and OE.CGA_TC_SVD ensure that the signatory gets a TOE example as authentic initialised and personalised SSCD.

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. The objectives OT.TOE_SSCD, OT.TOE_TC_SVD_Exp, OE.CGA_SSCD and OE.CGA_TC_SVD ensure that the signatory uses an authentic TOE, initialised and personalised for the signatory. The OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. The OE.SVD_Auth and the OE.CGA_QCert require the environment to ensure the authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. The OT.SCD_Unique provides that the signatory's SCD can practically occur just once.

The OE.Signatory ensures that the Signatory checks that the SCD, stored in the SSCD received from a 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). The 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 VAD confidential. The 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.

5.3.2.2 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 the Directive [1], recital (18). 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.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 the Directive [1], Annex III, paragraph 1, literal (c). The 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. The 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. The 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. The OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides the human interface for the user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. The 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. The OE.Signatory ensures also that the Signatory keeps his or her VAD 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. The 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. The 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. The OE.CGA_Qcert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA to generate a certificate. T.SVD_Forgery is addressed by OT.TOE_TC_SVD_EXP, that ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA_TC_SVD, that provides verification of SVD authenticity by the CGA.

5.3.2.3 Assumptions and Security Objective Sufficiency

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA with respect to the 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) and OE.CGA_TC_SVD (CGA trusted channel for SVD) which ensure the protection of the integrity of the SVD.

6 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.

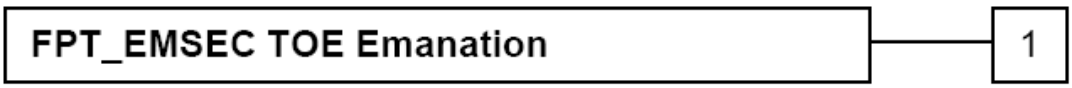
The section 6.1 describes the extended component FPT_EMSEC.1, section 6.2 describes the extended component FIA_API.1.

6.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



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.

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*].

6.2 Definition of the Family FIA_API

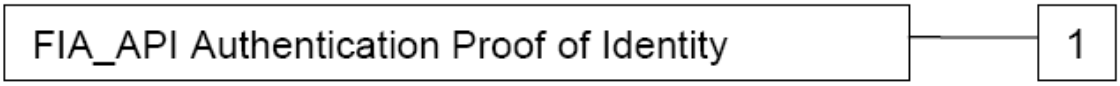
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:



FIA_API.1Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

7 IT Security Requirements

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

The Section 7.1 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 to a Security Target (ST).

The TOE security assurance requirements statement is given in section 7.2.

7.1 TOE Security Functional Requirements

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 ST. The following convention has been used for the generation of the SSCD core 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 by the PP authors are denoted as underlined 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 has been made by the PP authors is indicated as underlined 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.

For generation of the ST every operation performed in the ST is marked by segmented unterline. The application notes from the PP are kept in this ST. All required operations have been performed. Therefore the text from the original application note that contains just the request for performing the desired operations is omitted. The operations themselves are placed in the SFRs as well as in the application notes. All other text from the application notes from the PP are kept. All selections and assignments performed in the PP are kept in this ST. Assignments and selections performed in the PP or ST are

marked by PP or ST: assignment or selection: *operation to be performed*: chosen assignment or selection (e.g. PP: assignment: *list of cryptographic operations*: digital signature-generation or ST: assignment*: cryptographic key sizes:* 256 bit) . Descriptions of iterations and refinements in application notes of the PP are kept in this ST. Additional Application Notes added for this ST are marked as 'Application Note ST' without numbering.

7.1.1 Cryptographic support (FCS)

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 G&D_ECDSAKeyGen and specified cryptographic key sizes 256 bit that meet the following: [6].

Application note 1: The following operations have been performed:

PP: refinement: 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.

ST: assignment*: cryptographic key generation algorithm:* G&D_ECDSAKeyGen

ST: assignment*: cryptographic key sizes:* 256 bit

ST: assignment*: list of standards:* [6]

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 overwriting the key value with zero values that meets the following: none.

Application note 2: The following operations have been performed:

ST: assignment*: cryptographic key destruction method:* overwriting the key value with zero values

ST: assignment*: list of standards:* none

The cryptographic key SCD will be destroyed on demand of the Administrator during the Initialisation or Personalisation phase by overwriting the EEPROM containing the SCD with zero values. The deletion of the EEPROM is mandatory before the SCD/SVD pair is re-generated by the TOE within the Initialisation or Personalisation phase. Re-generation of the SCD/SVD pair is not possible during the usage phase.

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 in accordance with a specified cryptographic algorithm EC-DSA and cryptographic key sizes 256 bit that meet the following: [6].

Application note 3: The following operations have been performed:

PP: assignment: *list of cryptographic operations*: digital signature-generation

ST: *assignment: cryptographic algorithm:* EC-DSA

ST: *assignment: cryptographic key sizes*: 256 bit

ST: assignment: *list of standards:* [6]

7.1.2 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, R.Sigy
S.User	SCD / SVD Management	Authorised, not authorised
S.User	SVD Export	Authorised, not authorised
SCD	SCD Operational	No, yes
SCD	SCD identifier	Arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Application note 4: No additional objects or security attributes have been defined compared to the PP.

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

Application note 5: The following operations have been performed:

PP: assignment: *access control SFP*: SCD/SVD Generation SFP

PP: assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*: (1) subjects: S.User, (2) objects: SCD, SVD, (3) operations: generation of SCD/SVD pair.

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 to objects based on the following: the user S.User is associated with the security attribute "SCD / SVD Management".
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.
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.
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.

Application note 6: The following operations have been performed:

PP: assignment: *access control SFP*: SCD/SVD_Generation_SFP

PP: 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*: the user S.User is associated with the security attribute "SCD / SVD Management".

PP: assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*: S.User with the security attribute “SCD / SVD Management” set to “authorised” is allowed to generate SCD/SVD pair.

PP: assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*: none

PP: assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*: S.User with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair.

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 on (1) subjects: S.User, (2) objects: SVD (3) operations: export

Application note 7: The following operations have been performed:

PP: assignment: *access control SFP*: SVD_Transfer_SFP

PP: assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*: (1) subjects: S.User, (2) objects: SVD, (3) operations: export.

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 to objects based on the following: (1) the S.User is associated with the security attribute Role (2) the SVD.
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: (1) R.Admin is allowed to export SVD,
FDP_ACF.1.3/ SVD_Transfer_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ SVD_Transfer_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

Application note 8: The following operations have been performed:

PP: assignment: *access control SFP*: SVD_Transfer_SFP

PP: 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*: (1) the S.User is associated with the security attribute Role (2) the SVD.

PP: assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*: [selection: R.Admin, R.Sigy] is allowed to export SVD.

PP: assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*: none

PP: assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*: none.

ST: selection: *R.Admin, R.Sigy:* R.Admin;

Remark: There are no restrictions on reading the SVD, so reading the SVD is allowed for any user. The authentic export of the SVD that can be identified as 'authentic' by the CSP is restricted to R.Admin**.**

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

Application note 9: The following operations have been performed:

PP: assignment: *access control SFP*: Signature-creation_SFP

PP: assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*: (1) subjects: S.User, (2) objects: DTBS/R, SCD, (3) operations: signature-creation.

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

Application note 10: The following operations have been performed:

PP: assignment: *access control SFP*: Signature-creation_SFP

PP: 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*: (1) the user S.User is associated with the security attribute "Role" and (2) the SCD with the security attribute "SCD Operational".

PP: assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*: R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”.

PP: *assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects*: none

PP: assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*: S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “no”.

FDP_DAU.2/SVD Data Authentication with Identity of Guarantor

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1/SVD	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD.
FDP_DAU.2.2/SVD	The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note ST: The following operations have been performed:
ST: assignment: *list of objects or information types:* SVD
ST: assignment: *list of subjects:* CGA

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 the following objects: SCD.

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).

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

Application note 11: The following operations have been performed:
PP: selection: *allocation of the resource to, deallocation of the resource from*: de-allocation of the resource from
PP: assignment: *list of objects*: SCD

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 on all objects, based on the following attributes: integrity checked persistent stored data.
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.

Application note 12: The following operations have been performed:
PP: assignment: *integrity errors*: integrity error
PP: assignment: *user data attributes*: integrity checked persistent stored data

PP: assignment: *action to be taken*: (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error.

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 on all objects, based on the following attributes: integrity checked stored DTBS.
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.

Application note 13: 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).

The following operations have been performed:

PP: assignment: *integrity errors*: integrity error

PP: assignment: *user data attributes*: integrity checked stored DTBS

PP: assignment: *action to be taken*: (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error.

7.1.3 Identification and authentication (FIA)

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies:No dependencies.

FIA_API.1.1	The TSF shall provide a device authentication mechanism to prove the identity of the SSCD.

Application note ST: The following operations have been performed:

ST: assignment: *authentication mechanism:* device authentication mechanism

ST: assignment: *authorized user or rule:* SSCD

The TOE will authenticate itself as SSCD to the CGA.

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

Application note 14: The following operations have been performed:
PP: assignment: *list of TSF-mediated actions*: (1) Self test according to FPT_TST.1, (2) [assignment: list of additional TSF-mediated actions]
ST: assignment: *list of additional TSF-mediated actions:* Receiving DTBS.

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) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, (4) Receiving DTBS. 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 15: The following operations have been performed:
PP: assignment: *list of TSF-mediated actions*: (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]

ST: assignment: *list of additional TSF-mediated actions*: (3) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, (4) Receiving DTBS.

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 an administrator configurable positive integer within 1 and 10 unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD.

Application note 16: The following operations have been performed:
PP: assignment: *list of authentication events*: consecutive failed authentication attempts
PP: selection: *met, surpassed*: met
PP: assignment: *list of actions*: block RAD.
ST: selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]:* an administrator configurable positive integer within 1 and 10

7.1.4 Security management (FMT)

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

Application note 17: The following operations have been performed:

PP: assignment: *the authorised identified roles*: R.Admin and R.Sigy

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) none.

Application note 18: The following operations have been performed:
PP: assignment: *list of security management functions to be provided by the TSF*: (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].
ST: assignment: *list of other security management functions to be provided by the TSF:* none

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 the signature-creation function to R.Sigy.

Application note 19: The following operations have been performed:
PP: selection: *determine the behaviour of, disable, enable, modify the behaviour of*: enable

PP: assignment: *list of functions*: signature-creation function

PP: assignment: *the authorised identified roles*: R.Sigy

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 to restrict the ability to modify the security attributes SCD / SVD management to R.Admin.

Application note 20: The following operations have been performed:
PP: *assignment: access control SFP(s), information flow control SFP(s)*: SCD/SVD_Generation_SFP

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

PP: assignment: *list of security attributes*: SCD / SVD management

PP: assignment: *the authorised identified roles*: R.Admin

Application Note ST: Instead of assigning 'none' to 'other operations' the assignment has been deleted from the SFR for clarity.

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 to restrict the ability to modify the security attributes SCD operational to R.Sigy.

Application note 21: The following operations have been performed:
PP: assignment: *access control SFP(s), information flow control SFP(s)*: Signature-creation_SFP

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

PP: assignment: *list of security attributes*: SCD operational

PP: assignment: *the authorised identified roles*: R.Sigy

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_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

Application note 22: For 'SCD / SVD Management' only the secure values 'authorised' and 'not authorised' are accepted by the TOE. Both values are possible prior to conclusion of the personalisation phase and after conclusion of the personalisation phase. The default value is 'not authorised'. This value is secure, because with 'SCD / SVD Management' set to 'not authorised' no management of SCD and/or SVD can be performed. Especially, generation of a SCD/SVD pair is not possible in this state.
Only R.Admin prior to conclusion of the personalisation phase can set 'SCD / SVD Management' to 'authorised' and since authentication as Administrator is required for that, also the value 'authorised' is secure. After conclusion of the personalisation phase neither R.Admin nor R.Sigy can set 'SCD / SVD Management' to 'authorised' and with this the value 'authorised' is also secure in this life cycle phase.
For 'SCD operational' only the secure values 'yes' and 'no' are accepted. SCD operational is set to 'no' as long as the VAD is still in its transport state. With SCD operational set to 'no' no signature can be generated so this value is secure. SCD operational can only be set to 'yes' after conclusion of the personalisation phase and only be R.Sigy. Since an authentication by RAD is required to set SCD operational to 'yes', also this value is secure.

The following operations have been performed:
PP: assignment: *list of security attributes*: SCD / SVD Management and SCD operational.

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 and Signature-creation_SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.

Application note 23: The following operations have been performed:
PP: assignment: *access control SFP, information flow control SFP*: SCD/SVD_Generation_SFP and Signature-creation_SFP

PP: selection, chose one of: *restrictive, permissive, [assignment: other property]*: restrictive

PP: assignment: *the authorised identified roles*: R.Admin

Application Note ST: The TSF allow the R.Admin to specify alternative initial values but the only possible alternative values would violate other SFRs and therefore the possibility to specify alternative initial values is of no practical relevance for this TOE.

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 the 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.

Application note 24: The following operations have been performed:

PP: assignment: *rules for setting the values of security attributes*: (1) If S.Admin successfully generates an SCD/SVD pair without the 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.

Application Note ST: The TOE does only allow generation of the SCD/SVD by S.Admin before conclusion of the personalisation phase (S.Sigy is only present after conclusion of the personalisation phase). After conclusion of the personalisation phase neither S.Admin nor S.Sigy are allowed to generate or re-generate the SCD/SVD. Therefore FMT_MSA.4.1 (1) is only relevant before the conclusion of the personalisation phase and FMT_MSA.4.1. (2) is not relevant for the TOE.

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 the RAD to R.Admin.

Application note 25: The following operations have been performed:
PP: selection: *change_default, query, modify, delete, clear, [assignment: other operations]*: create (Remark: i.e. assignment for other operations)

PP: assignment: list *of TSF data*: RAD

PP: assignment: *the authorised identified roles*: R.Admin

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 the RAD to S.Sigy.

Application note 26: The following operations have been performed:
PP: selection: *change_default, query, modify, delete, clear, [assignment: other operations]*: modify [assignment: other operations]

PP: assignment: *list of TSF data*: RAD

PP: assignment: *the authorised identified roles*: S.Sigy

Application note 27: Instead of assigning 'none' to 'other operations' the assignment has been deleted from the SFR for clarity.

7.1.5 Protection of the TSF (FPT)

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non useful information enabling access to RAD and SCD.
FPT_EMSEC.1.2	The TSF shall ensure S.Offcard are unable to use the following interface contacts VCC, GND, IO to gain access to RAD and SCD.

Application note 28: The following operations have been performed:
PP: assignment: *list of types of TSF data*: RAD
PP: assignment: *list of types of user data*: SCD
PP: assignment: *list of types of TSF data*: RAD
PP: assignment: *list of types of user data*: SCD
ST: *assignment: types of emissions*: information about IC power consumption and command execution time
ST: *assignment: specified limits:* non useful information
ST: *assignment: type of users:* S.Offcard
ST: *assignment: type of connection:* contacts VCC, GND, IO

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.

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) inconsistencies in the calculation of the signature.

Application note 29: The following operations have been performed:
PP: assignment: *list of types of failures in the TSF*: (1) self-test according to FPT_TST fails, (2) [assignment: list of other types of failures in the TSF].
ST: *assignment: list of other types of failures in the TSF:* inconsistencies in the calculation of the signature

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.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist tampering of the physical operating conditions voltage supply, clock frequency and temperature beyond the valid limits to the IC by responding automatically such that the SFRs are always enforced.

Application note 30: The following operations have been performed:

ST: assignment: *physical tampering scenarios:* tampering of the physical operating conditions voltage supply, clock frequency and temperature beyond the valid limits
ST: assignment: *list of TSF devices/elements:* IC

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

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 during initial start-up, periodically during normal operation, at the condition Reset of the TOE to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application note 31: The following operations have been performed:
PP: selection: *[assignment: parts of TSF], the TSF*: the TSF
PP: selection: *[assignment: parts of TSF data], TSF data*: TSF data
PP: selection: *[assignment: parts of TSF], TSF*: stored TSF executable code (Remark: i.e. assignment to parts of TSF)

ST: selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*: during initial start-up, periodically during normal operation, at the condition
ST: *assignment: conditions under which self test should occur:* Reset of the TOE

7.1.6 Trusted Path/Channels (FTP)

FTP_ITC.1/SVD Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies:No dependencies.

FTP_ITC.1.1/SVD	The TSF shall provide a communication channel between itself and another trusted IT product CGA that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SVD	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SVD	The TSF or the CGA shall initiate communication via the trusted channel for Data Authentication with Identity of Guarantor according to FDP_DAU.2/SVD.

Application note ST: The following operations have been performed:

ST: Refinement: The trusted IT product in FTP_ITC.1.1 has been refined as CGA.

ST: selection: *the TSF, another trusted IT product*: another trusted IT product

ST: assignment: *list of functions for which a trusted channel is required*: Data Authentication with Identity of Guarantor according to FDP_DAU.2/SVD

7.2 TOE Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.4 Complete functional specification

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

Table 2: Assurance Requirements: EAL4 augmented with AVA_VAN.5

8 TOE Summary Specification

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

8.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users (Administrator, Signatory). After activation or reset no user is authenticated. The Administrator can authenticate himself using symmetric device authentication. The Signatory can authenticate himself using the signature PIN. After up to 10 unsuccessful consecutive authentication attempts the signature PIN is permanently blocked. The administrator defines the maximum number of attempts.

The access control mechanisms ensure that only the Administrator can generate the signature key pair or export the public signature key in an authentic way for certification or store a transport value for the signature PIN. In addition, only the Administrator can store the certificate or certificate information for the public signature key on the TOE. The access control mechanisms also ensure that only the Signatory can set and change the signature PIN or generate electronic signatures using the private signature key.

The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

This security function covers the following SFRs: FDP_ACC.1, FDP_ACF.1, FIA_UID.1, FIA_UAU.1, FIA_AFL.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1

8.2 SF_AssetProtection

When the private signature key or the signature PIN are no longer needed in the internal memory of the TOE for calculations these parts of the memory are overwritten.

The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets residing on the TOE as well as temporarily stored hash values for data that is intended to be signed.

The TOE hides information about IC power consumptions and command execution time, to ensure that no confidential information can be derived from this data.

This security function covers the following SFRs: FDP_RIP.1, FDP_SDI.2, FPT_EMSEC.1

8.3 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. The TOE is resistant to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

This security function covers the following SFRs: FPT_PHP.1, FPT_PHP.3, FPT_FLS.1, FPT_TST.1

8.4 SF_KeyManagement

The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [12]. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying IC.

The TOE supports onboard generation of corresponding EC-DSA keypairs with key length 256 bit. For this the TOE uses random numbers generated by its K4 (high) deterministic random number generator.

The TOE supports overwriting the signature keypair stored in the EEPROM with zero values prior to conclusion of the Personalisation Phase.

This security function covers the following SFRs: FCS_CKM.1, FCS_CKM.4

8.5 SF_SignatureGeneration

The TOE supports calculations with elliptic curves defined over a field F(p) and with lengths of the parameters p and q of 256 bit. In addition, the TOE supports calculations of hash values according to SHA-2 (256 bit). Based on these calculations the TOE supports generation of EC-DSA signatures according to EN14890 [7].

This security function covers the following SFRs: FCS_COP.1

8.6 SF_TrustedCommunication

The TOE supports the establishment of a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity. The mutual authentication is based on a challenge response protocol using the Triple DES algorithm with key sizes of 192 bit. This algorithm is also used for encryption and integrity protection of the communication data. Via this trusted channel/path the Administrator can authentically export the public signature key for certification and import the certificate or certificate information for the public signature key.

This security function covers the following SFRs: FIA_API.1, FDP_DAU.2, FTP_ITC.1

8.7 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

Table 6.2: References of Assurance Measures

Assurance Measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation..
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

9 Rationale

9.1 Security Requirements Rationale

9.1.1 Security Requirement Coverage

	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	OT.TOE_SSCD	OT.TOE_TC_SVD_EXP
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_ACF.1/ SCD/SVD_Generation_SFP	X	X											
FDP_ACF.1/ SVD_Transfer_SFP													X
FDP_ACF.1/Signature-creation_SFP	X						X						
FDP_RIP.1					X		X						
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						

	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	OT.TOE_SSCD	OT.TOE_TC_SVD_EXP
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							
FDP_DAU.2/SVD													X
FIA_API.1												X	
FTP_ITC.1/SVD													X

Table 3: Functional Requirement to TOE security objective mapping

9.1.2 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 SCD usage is ensured by access control FDP_ACC.1/Signature-creation_SFP, FDP_ACF.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 the Directive [1], Annex III, article 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).

The 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. The SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS 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 requires 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.

OT.TOE_SSCD (Protection of VAD provided by SCA) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA_API.1 (Authentication Proof of Identity).

OT.TOE_TC_SVD_EXP (TOE trusted channel for SVD) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- 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.

– FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
– FTP_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

9.2 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.

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

Requirement	Dependencies	Fulfilled
FDP_ACF.1/ SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP, FMT_MSA.3
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
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.
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FIA_API.1	No dependencies	n. a.

Requirement	Dependencies	Fulfilled
FTP_ITC.1/SVD	No dependencies	n. a.
FDP_RIP.1	No dependencies	n. a.
FDP_SDI.2/Persistent	No dependencies	n. a.
FDP_SDI.2/DTBS	No dependencies	n. a.
FPT_EMSEC.1	No dependencies	n. a.

Table 4: Functional Requirements Dependencies

9.3 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.

10 Acronyms

CC	Common Criteria
CGA	Certification generation application
DTBS	Data to be signed
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
(S)RAD	(Signatory's) 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
(S)VAD	(Signatory's) Verification authentication data

11 Conventions and Terminology

11.1 Conventions

The document follows the rules and conventions laid out in Common Criteria 3.1, part 1 [2], Annex B “Specification of Protection Profiles”.

11.2 Terminology

Administrator means an user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control, and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data is information used to verify the claimed identity of a user. The TOE provides role-based authentication of the roles Admin and Signatory without further identification of the user.

Certificate means an electronic attestation, which links the SVD to a person and confirms the identity of that person (as defined in the Directive [1], article 2, clause 9).

Certificate info means information associated with a SCD/SVD pair that consists either:

a signer's public key certificate, or

one or more hash values of a signer's public key certificate together the identifier of the hash function used to compute these hash values, and some information which allows the signer to disambiguate between several signers certificates."

Certification generation application (CGA) means a collection of application elements which receives the SVD from the SSCD for generation of the certificate, obtaining the data included in the certificate and creating the signature of the certificate.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (as defined in the Directive [1], article 2(11))

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed or its unique representation (DTBS/R) means the 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.

Directive: 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] is also referred to as the 'Directive' in the remainder of the PP.

Notified body: The Member States shall notify to the Commission and the other Member States about the national bodies (referred as notified bodies in this PP) which are responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4) (cf. Directive [1], article 11(1b)). Note the bodies referred to in Article 3(4) determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III.

Qualified certificate means a certificate, which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1] (cf. the Directive [1], article 2.10).

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by an SSCD according to the Directive [1], article 5, paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

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

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (The term SSCD is defined in the Directive [1], article 2.5 and 2.6).

Signatory means a person who holds an SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents (as defined in the Directive [1], article 2.3).

Signature attributes means additional information that is signed together with the user message.

Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements

(a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision,

(b) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intent to sign,

(c) to include the digital signature generated by the TOE into the electronic signature.

Signature-creation-data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (as defined in the Directive [1], article 2.4). In the context of this PP the SCD means the private key used to create the signature.

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (as defined in the Directive [1], article 2.7). In the context of this PP the SVD means the public key corresponding to the SCD implemented on the SSCD and used to verify the signature.

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides an SSCD to subscribers. For a Type 3 SSCD the SSCD provision service runs a collection of application elements which installs the SRAD in the SSCD, requests the generation of one or more SCD / SVD key pairs by the SSCD, requests the SVD from the SSCD, and provides the SVD to the CGA to create the certificate or certificates by the appropriate Certification Authorities. In most cases the SSCD provision service will be a part of the Certification-service-provider.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

12 References

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

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

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

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

[5] Protection Profile Secure Signature-Creation Device Type 3, Version 0.93 CC-V3.1

[6] Bundesgesetzblatt für die Republik Österreich, Jahrgang 2008, ausgegeben am 7. Jänner 2008, Teil II, Signaturverordnung 2008 - SigV 2008

[7] EUROPEAN STANDARD, EN 14890-1:2008, Application Interface for smart cards used as secure signature creation devices – Part 1: Basic services

[8] Certification Report BSI-DSZ-CC-0466-2008 for Smart Card Controller P5CC052V0A with specific IC Dedicated Software from NXP Semiconductors Germany GmbH, 24.06.2008

[9] Security Target Lite, P5CC052V0A, Rev. 1.1, 16.04.2008.

[10] Smart Card IC Platform Version 1.0, Juli 2001, BSI-PP-0002-2001

[11] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

[12] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.1999

[13] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-007-09-001.

[14] Protection Profile - Secure Signature-Creation Device Type 3 with Trusted Communication SSCD/CGA, Version 0.5