Security Target Lite STARCOS 3.5 ID ECC C1R

Version 2.3/21.03.13

Author: Giesecke & Devrient GmbH
Document status: Public

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

Content

1 Introduction

1.1 TOE Reference

This document refers to the following TOE(s):

1) STARCOS 3.5 ID ECC C1R

1.2 ST Reference and ST Identification

Title: Security Target Lite STARCOS 3.5 ID ECC C1R

Version Number/Date: Version 2.3/21.03.13

Origin: Giesecke & Devrient GmbH

TOE: STARCOS 3.5 ID ECC C1R

1.3 TOE Overview

The aim of this document is to describe the Security Target for STARCOS 3.5 ID ECC C1R. In the following chapters STARCOS 3.5 ID ECC C1R stands for the Target of Evaluation (TOE).

STARCOS 3.5 ID ECC C1R is a smart card and is intended to be used as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC[1] [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 **The Directive** have been mapped into a Protection Profile (PP) for Secure Signature Creation Devices of Type 3[2]. The 'Security Target STARCOS 3.5 ID ECC C1R' is strictly conformant to the “Protection profiles for Secure signature creation device with generation of the signature key on the device” [5]. When operated in a secure environment for signature creation a signer may use an SSCD that fulfils only these core security requirements to create an advanced electronic signature[3]. As the TOE can be operated in other environments the security requirements of the non certified protection profile “Protection profiles for secure signature creation

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

[2] An SSCD that can create its own SCD/SVD is known as an SSCD Type 3 to be distinguished from type 1 and type 2 as defined in the Protection Profile Secure Signature-Creation Device Type 3 [16].

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

device - Part 5: Device with key generation and trusted communication with signature creation application" [16] are included in this Security Target. Furthermore the TOE provides trusted communication with the certificate generation application, therefore also the security requirements of the non certified protection profile "Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application" [15] were included in this Security Target. These Protection Profiles claim conformance to the "Protection profiles for Secure signature creation device – Part 2: Device with key generation" [5].[4]

STARCOS 3.5 ID ECC C1R comprises:

- the STARCOS 3.5 ID operating system,
- the hardware platform Infineon M7820 (Certificate: BSI-DSZ-CC-0813-2012) with the following configurations according [9]:
    - NVM: 36 kByte up to 128 kByte
    - ROM: 280 kByte
    - XRAM: 8 kByte
    - SCP: Accessible
    - Crypto2304T: Accessible
    - Interfaces: ISO/IEC 7816 and/or ISO/IEC 14443

  The sales names of the TOE hardware platform [9] and the corresponding TOE names of STARCOS 3.5 ID ECC C1R are listed below:

sales name of M7820 [9]	**TOE name of STARCOS 3.5 ID ECC C1R**
SLE78CLX360P	STARCOS 3.5 ID ECC C1R/360
SLE78CLX800P	STARCOS 3.5 ID ECC C1R/800
SLE78CLX1280P	STARCOS 3.5 ID ECC C1R/1280

- the TOE documentation
    - Guidance Documentation STARCOS 3.5 ID ECC C1 – Main Document
    - Guidance Documentation for the Initialisation Phase STARCOS 3.5 ID ECC C1
    - Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID ECC C1
    - Guidance Documentation for the Usage Phase STARCOS 3.5 ID ECC C1
    - Generic Application of STARCOS 3.5 ID ECC C1R, which specifies the file system

[4] See CC part 1 chapter 8.5

- the Smart Card Application Verifier[5], which verifies the conformance of the installed file system with the Generic Application,
- the signature application, which is a file system configured according the Generic Application.

STARCOS 3.5 ID 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 upto 521 bit and based on RSA with a key length of upto 4096 bit. The EU compliant Electronic Signature Application is designed for the creation of legally binding Qualified Electronic Signatures as defined in **The Directive**. The signature application is compliant to EN 14890 “Application Interface for smart cards used as Secure Signature Creation Devices”. The various features of STARCOS 3.5 allow for additional applications like ID applications compliant to CEN/TS 15480 “Identification card systems – European Citizen Card”.
Beside contact based communication according Part 3 of ISO/IEC 7816 STARCOS 3.5 ID supports contactless communication according ISO/IEC 14443. STARCOS 3.5 ID ECC C1R can be configured for sole contact based communication, sole contactless communication and for dual interface supporting contact based and contactless communication.
The software part of the TOE is implemented on the certified M7820 A11 from Infineon [9]. So the TOE consists of the software part and the underlying hardware. The crypto library for Crypto@2304T provided with the underlying hardware is not used in this composite TOE. The software part of the calculations based on elliptic curves and RSA is implemented in the operating system. The Security Target (Lite) of the hardware platform [9] is compliant to the BSI-CC-PP-0035 [10].

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 **FIA_API.1 (**Authentication Proof of Identity*)*.

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

- AVA_VAN.5

as stated in [5].

[5] The Smart Card Application Verifier is not part of the TOE delivery. It is solely used by the OS Developer for the correct installation of the TOE and therefore of no use for the Card Initialising and Personalisation facility.

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

In the following the TOE is described according the Protection profiles for Secure signature creation devices [5], [5a], [15], [16] and the corresponding overview document [14].

2.1 Operation of the TOE

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

- The signing environment where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature[6]. The TOE provides the functionality to communicate with the SCA through a trusted channel to ensure the integrity of the DTBS respective DTBS/R.
- The preparation environment, where it interacts with a certification service provider through a certificate-generation application (CGA) to obtain a certificate for the signature validation data (SVD) corresponding with signature creation data (SCD) the TOE has generated. The TOE offers the CGA the possibility to export the SVD through a trusted channel. The CGA has to choose the trusted channel for the export to be able to check the authenticity of the SVD. The initialization environment interacts further with the TOE to personalize it with the initial value of the reference-authentication data (RAD).
- The management environments where it interacts with the user or an SSCD-Provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

The signing environment, the management environment and the preparation environment are secure and protect data exchanged with the TOE. Figure 4 and Figure 5 in prEN14169-1 "Protection Profile for Secure Signature Creation Device - Part 1: Overview” [14] illustrates the operational environments.

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

The TOE stores signature creation data and reference authentication data. The TOE may store multiple instances of SCD. In this case the TOE will provide a function to identify each SCD and the signature creation application (SCA) can provide an interface to the signer to select an SCD for use in the signature creation function of the SSCD. The TOE protects the confidentiality of the SCD and restricts its use in signature creation to its signatory. The digital signature created with the TOE is a *qualified electronic signature* as defined in **The Directive** if the certificate for the SVD is a qualified certificate (Annex I).

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

The TOE stores signatory reference authentication data to authenticate a user as its signatory. The RAD is a password e.g. PIN. The TOE protects the confidentiality and integrity of the RAD. The TOE receives the verification authentication data (VAD) from the signature creation application. If the signature creation application handles requesting obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

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

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

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

2.2 Target of Evaluation (TOE)

The TOE is realised by a smartcard, comprising the certified chip, the operating system and the QES-application.

The operating system 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 an ID application, 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.

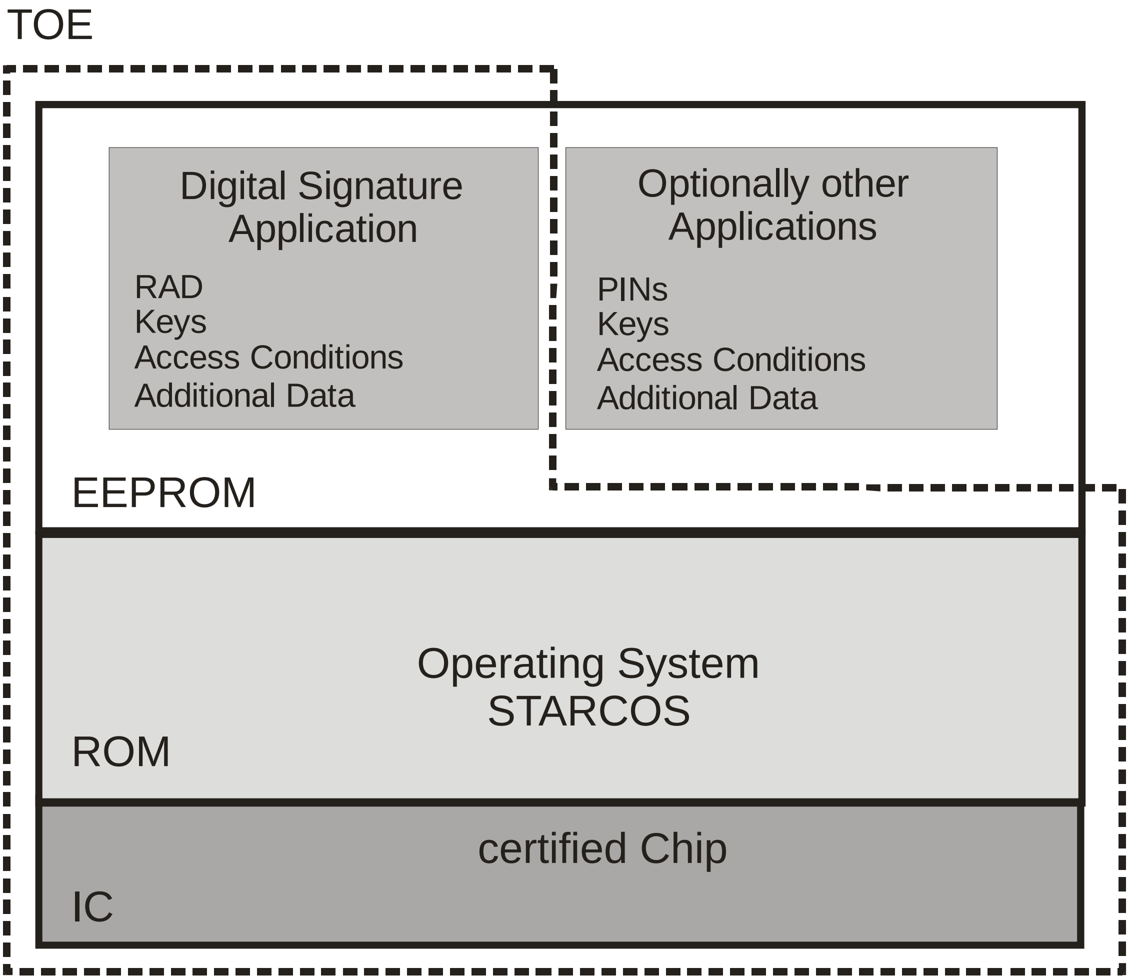


Figure 1: TOE description (after installation)

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.

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

The TOE provides the following functions:

(1) to generate signature creation data (SCD) and the correspondent signature-verification data (SVD),
(2) to export the SVD, for certification the CGA has to choose the trusted channel for the export,
(3) to prove the identity as SSCD to external entities,
(4) to, optionally, receive and store certificate info,
(5) to switch the TOE from a non-operational state to an operational state, and
(6) if in an operational state, to create digital signatures for data with the following steps:
  (a) select an SCD if multiple are present in the SSCD,
  (b) authenticate the signatory and determine its intent to sign,
  (c) receive data to be signed or a unique representation thereof (DTBS/R),
  (d) apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

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

The TOE is prepared for the signatory's use by

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

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

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

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

2.3 TOE life cycle

2.3.1 General

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

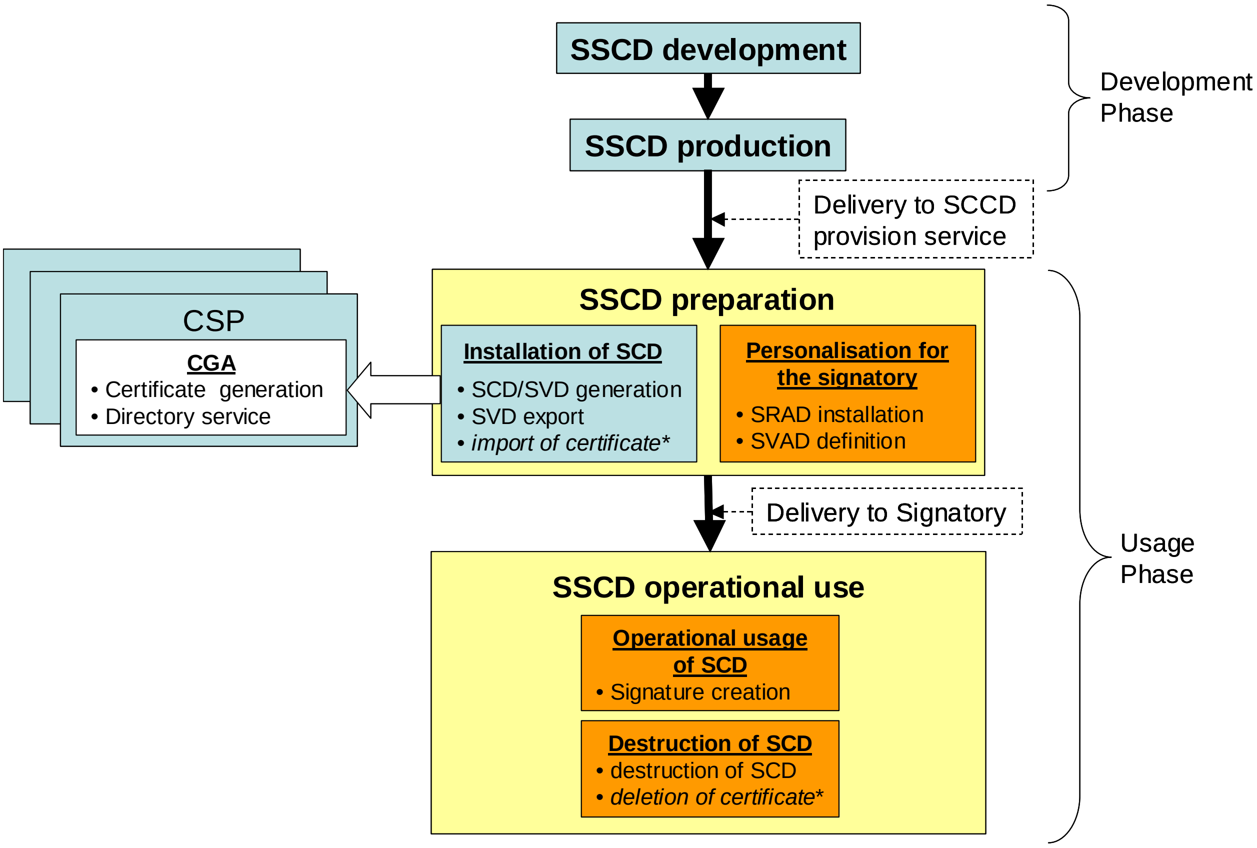


Figure 2: Typical TOE life cycle[7]

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

2.3.2 Preparation stage

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

(1) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.

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

(2) Perform the initialisation, i.e. load secured data structures representing the file system of the signature application onto the card.

(3) Generate a PIN, store this data as RAD in the TOE and prepare information about the VAD for delivery to the legitimate user.

(4) Initialization of the security functions in the TOE for the identification as SSCD, the proof of this SSCD identity to external entities, and the protected export of the SVD.

(5) The generation of the (qualified) certificate containing among others (cf. [1], Annex II):

   a. the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE,

   b. an indication of the beginning and end of the period of validity of the certificate.

(6) Optionally, present certificate info to the SSCD.

(7) Link the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE.

(8) Deliver the TOE and the accompanying VAD info to the legitimate user.

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

Data required for inclusion in the SVD certificate at least includes (**Annex** II):

- The SVD;
- The name of the signatory either

   (a) A legal name, or

   (b) A pseudonym together with an indication of this fact.

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

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

Before generating the certificate signature the CGA verifies the sender and the received SVD by:

- establishing the sender as genuine SSCD and the identity of the TOE as SSCD;

- establishing the integrity of the SVD to be certified as sent by the originating SSCD;
- establishing that the originating SSCD has been personalized for the applicant for the certificate as legitimate user;
- establishing the correspondence between SCD implemented in the SSCD and the received SVD, and

an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in this ST.

2.3.2.1 Delivery of ROM-Mask and initialisation data

As shown in the following figure, the Software part of the TOE consists of the operating system located in the ROM of the IC and the File System located in the EEPROM. Parts of the operating system may also reside in the EEPROM. The operating system developer (i.e. G&D) sends a representation of the operating system together with secret data allowing secure loading of initialisation data to the Chip Manufacturer. 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 point of delivery may be before or after initialisation of the TOE. The development phase may therefore end before or after the initialisation of the TOE. In case the initialisation is performed by G&D it is part of the development phase. In case the initialisation is not performed by G&D the point of delivery of the TOE is before the initialisation that will take place at another site in the form of modules.

The Card Initialising Facility performs the initialisation, optionally the inlay embedding and production of the cards possibly at different sites. Afterwards the cards are delivered to the personalising facility. The delivery of the TOE to the SSCD provision service happens either at the delivery to the initialisation site, or the inlay embedding site, or the card production site or the personalisation site. The TOE can therefore be delivered either as Module, inlay or card to SSCD provision service.

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.

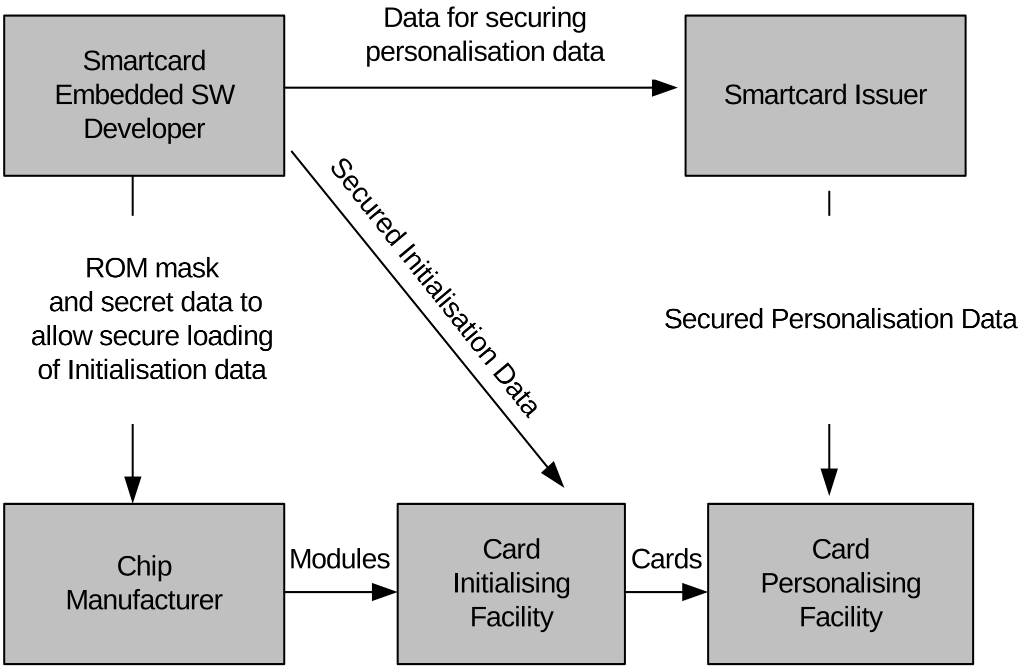

Smartcard Embedded SW Developer
Data for securing personalisation data
Smartcard Issuer
Secured Initialisation Data
ROM mask and secret data to allow secure loading of Initialisation data
Secured Personalisation Data
Chip Manufacturer
Modules
Card Initialising Facility
Cards
Card Personalising Facility

Figure 3: ROM Mask and initialisation data delivery

2.3.3 Operational use stage

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

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

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

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

The TOE supports functions to generate additional signing keys and supports functions to securely obtain certificates for the new keys. For an additional key the signatory may be allowed to choose the kind of certificate (qualified, or not) to obtain for the SVD of the new key. The signatory may also be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[8]. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures.

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

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

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target is Common Criteria version 3.1 Revision 4 [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 claims strict conformance to the Common Criteria Protection Profile – Protection profiles for Secure signature creation device – Part 2: Device with key generation [5].

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

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

4 Security Problem Definition

The 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 security environment.

Assets and objects:

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS-representation: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.
4. Signature creation function of the TOE to create digital signature for the DTBS/R with the SCD.

Users and Subjects acting for users:

1. User: End user of the TOE who can be identified as Administrator or Signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
2. Admin. User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
3. Signatory: User who hold the TOE and uses it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents

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

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 forges the SVD presented by the CSP 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 SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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*

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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. **the directive**, 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. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[9]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The

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

SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

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

4.3 Assumptions

A.CGA *Trustworthy certificate generation application*

The CGA protects the authenticity of the signatory’s name or pseudonym and the SVD in the (qualified) certificate by an advanced 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

5.1.1 Security Objectives for the SSCD with key generation [5]

All security objectives for the TOE from “Protection profiles for Secure signature creation device – Part 2: Device with key generation” (see [5]) are included in this security target without modification.

OT.Lifecycle_Security *Lifecycle security*

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

Application note 1: The TOE may contain more than one set of SCD. In case of re-generation the SCD is destroyed. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_ Auth_Gen Authorized SCD/SVD generation

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

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 shall practically occur only once and shall not be reconstructable 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 in creating an electronic signature creation with the SCD.

OT.SCD_Secrecy *Secrecy of the signature creation data*

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

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

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

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

OT.DTBS_Integrity_TOE *DTBS/R integrity inside the TOE*

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

OT.EMSEC_Design *Provide physical-emanation security*

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

OT.Tamper_ID *Tamper detection*

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

OT.Tamper_Resistance *Tamper resistance*

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

5.1.2 Security Objectives for the trusted communication with CGA [15]

All security objectives for the TOE from “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application” (see [15]) are included in this security target without modification.

OT.TOE_SSCD_Auth *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.

5.1.3 Security Objectives for the trusted communication with SCA

The following objectives are based on the corresponding ones of “Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature creation application” (see [16]), but were modified to allow the card issuer to configure the existence of these trusted channels.

OT.TOE_confTC_VAD_Imp *Optional trusted channel of TOE for VAD import*

During intialisation the TOE shall be configurable to provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

OT.TOE_confTC_DTBS_Imp *Optional trusted channel of TOE for DTBS import*

During intialisation the TOE shall be configurable to provide a trusted channel to the SCA to detect alteration of the DTBS-representation received from the SCA. The TOE must not generate digital signatures with the SCD for altered DTBS.

5.2 Security Objectives for the Operational Environment

5.2.1 Security Objectives regarding the SSCD with key generation

All security objectives for the operational environment from “Protection profiles for Secure signature creation device – Part 2: Device with key generation” (see [5]) are included in this security target, except the following three:

1) OE.SSCD_Prov_Service was replaced by the security objective OE.Dev_Prov_Service (see chapter 5.2.2).
2) OE.HID_VAD was replaced by the security objective OE.HID_confTC_VAD_Exp (see chapter 5.2.3).
3) OE.DTBS_Protect was replaced by the security objective OE.SCA_confTC_DTBS_Exp (see chapter 5.2.3).

The following objectives are taken from “Protection profiles for Secure signature creation device – Part 2: Device with key generation” (see [5]) without modification.

OE.SVD_Auth *Authenticity of the SVD*

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

OE.CGA_QCert *Generation of qualified certificates*

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

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

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

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

The Signatory shall use a trustworthy SCA that

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

OE.Signatory *Security obligation of the Signatory*

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

5.2.2 Security Objectives regarding the trusted communication with CGA

All security objectives for the operational environment from “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application” (see [15]) were included in this security target without modification.

OE.Dev_Prov_Service *Authentic SSCD provided by SSCD Provisioning Service*

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

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

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and this identity is linked to the legitimate holder of the device as applicant for the certificate.

OE.CGA_TC_SVD_Imp CGA *trusted channel for SVD import*

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by OE.SSCD_Prov_Service [5] except the additional intialisation of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the SSCD Provisioning Service service as described in OE.Dev_Prov_Service. Therefore this ST substitutes OE.SSCD_Prov_Service of [5] by OE.Dev_Prov_Service of [15] allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational envirnment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core PP SSCD KG [5].

5.2.3 Security Objectives for the trusted communication with SCA

The following objectives are based on the corresponding ones of “Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature creation application” (see [16]), but were modified to allow the card issuer to configure the existence of these trusted channels.

OE.HID_confTC_VAD_Exp *Optional trusted channel of HID for VAD export*

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel if available.

OE.SCA_confTC_DTBS_Exp *Optional trusted channel of SCA for DTBS export*

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. If available the SCA uses the trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS-representation cannot be altered undetected in transit between the SCA and the TOE.

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_Auth_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_confTC_VAD_Imp	OT.TOE_confTC_DTBS_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_confTC_VAD_Exp	OE.DTBS_Intend	OE.SCA_confTC_DTBS_Exp	OE.Signatory
T.SCD_Divulg					X																			
T.SCD_Derive		X				X																		
T.Hack_Phys					X				X	X	X													
T.SVD_Forgery				X											X		X		X					
T.SigF_Misuse	X						X	X				X	X								X	X	X	X
T.DTBS_Forgery								X					X									X	X	
T.Sig_Forgery			X			X												X						
P.CSP_QCert	X			X										X		X		X						
P.QSign						X	X											X				X		
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X			X	X	X	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	X	X	X	X
A.CGA																		X	X					
A.SCA																						X		

Table 1: Security problem definition to security objectives mapping

5.3.2 Security Objectives Sufficiency

5.3.2.1 Sufficiency regarding the SSCD with key generation [5]

5.3.2.1.1 Policies and Security Objective Sufficiency

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

5.3.2.1.2 Threats and Security Objective Sufficiency

T.SCD_Divulg *(Storing,copying, and releasing of the signature creation data)* addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of **The Directive**. This threat is countered by **OT.SCD_Secrecy**, which assures the secrecy of the SCD used for signature creation.

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

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

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

5.3.2.1.3 Assumptions and Security Objective Sufficiency

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

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

5.3.3 Sufficiency regarding the trusted communication with CGA [15]

T.SVD_Forgery (*Forgery of the signature-verification data*) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP. Additionally T.SVD_Forgery is addressed by OT.TOE_TC_SVD_Exp, which 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_Imp, which provides verification of SVD authenticity by the CGA.

P.CSP_QCert (*CSP generates qualified certificates*) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, 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_Auth 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_Auth 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 Annex III of the Directive. The paragraph 1(a) of Annex III is ensured by OT.SCD_Unique requireing that the SCD used for signature generation can practically occurs only once. The OT.SCD_Secrecy OT.Sig_Secure and OT.EMSEC_Design and OT.Tamper_Resistance adress the secrecy of the SCD (cf. paragraph 1(a) of Annex III). OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE. OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III by the requirements to ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III as the TOE must not alter the DTBS/R. The usage of SCD under sole control of the signatory is ensured by OT.Lifecycle_Security, OT.SCD/SVD_Gen and OT.Sigy_SigF.

OE.Dev_Prov_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA_SSCD_Auth and the received SVD is sent by this SSCD as required by OE.CGA_TC_SVD_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

5.3.4 Sufficiency for the trusted communication with SCA

T.SigF_Misuse (*Misuse of the signature creation function of the TOE*) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create a digital signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of **Annex** III. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of OT.TOE_confTC_DTBS_Imp (Optional trusted channel of TOE for DTBS) and OE.SCA_confTC_DTBS_Exp (Optional trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. As the SCA provides a human interface for user authentication, OE.HID_confTC_VAD_Exp (Optional trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. If available the HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_confTC_VAD_Exp (Optional trusted channel of HID for VAD) and OT.TOE_confTC_VAD_Imp (Optional trusted channel of TOE for VAD). OE.Signatory ensures that the Signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the Signatory becomes control over the SSCD. OE.Signatory ensures also that the Signatory keeps his or her VAD confidential.

T.DTBS_Forgery (*Forgery of the DTBS-representation*) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_confTC_DTBS_Imp (Optional trusted channel of TOE for DTBS) and OE.SCA_confTC_DTBS_Exp (Optional trusted channel of SCA for DTBS), which ensure that the DTBS-representation cannot be altered undetected in transit between the SCA and the TOE and if available using the corresponding trusted channel. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE ensuring the integrity of the DTBS-representation inside the TOE.

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, that ensure the aspects of signatory’s sole control over and responsibility for the digital signatures generated with the TOE. OE.Dev_Prov_Service ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory’s SCD can practically occur just once.

OE.Signatory ensures that the Signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the Signatory becomes into sole control over the SSCD). The TOE security feature addressed by the security objectives OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp supported by OE.Dev_Prov_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA_SSCD_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA_TC_SVD_Imp. OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite

OE.Signatory ensures that the Signatory keeps his or her SVAD confidential. The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_confTC_VAD_Exp and OT.TOE_confTC_VAD_Imp. OE.DTBS_Intend, OT.DTBS_Integrity_TOE, OE.SCA_confTC_DTBS_Exp and OT.TOE_confTC_DTBS_Imp 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.

6 Extended Component Definition

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations.

The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the *Protection Profile Secure Signature Creation Device – Part 2: Device with key generation* [5], chapter 9. The section 6.1 describes the extended component FPT_EMS.1, section 6.2 describes the extended component FIA_API.1.

6.1 FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

FPT_EMS TOE Emanation
1

Component levelling:

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.2 Definition of the Family FIA_API

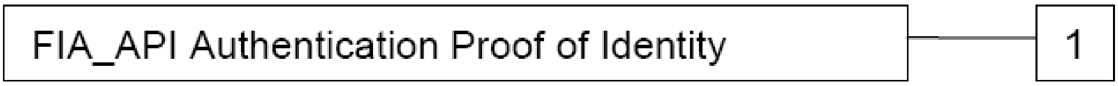
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external 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.1 Authentication 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.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

7 IT Security Requirements

7.1 General

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

Section 6 describes the extended components FPT_EMS.1 and FIA_API.1. The Section 7.2 provides the security functional requirements. All security functional requirements of “Protection profiles for Secure signature creation device – Part 2: Device with key generation” (see [5]) were taken without modifications beside operations for assignment, selection and refinement. All additional security functional requirements (FIA_API.1, FDP_DAU/SVD, FTP_ITC.1/SVD) from “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application” (see [15]) were included in this security target without modifications. The additional security functional requirements FTP_ITC.1/Conf_VAD and FTP_ITC.1/Conf_DTBS are based on the corresponding ones of “Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature creation application” (see [16]), but were modified to allow the card issuer to configure the existence of these trusted channels. The remaining additional security functional requirement from [16], FDP_UIT.1/DTBS, was not included into this security target also to enable the card issuer to configure the existence of these trusted channels.

The TOE security assurance requirements statement is given in section 7.3.

7.2 TOE Security Functional Requirements

7.2.1 Use of requirement specifications

Common Criteria allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of part 2 of the CC. Each of these operations is used in this ST. The following convention has been used for the generation of this ST:

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 an application note. 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 <u>underlined</u> text and the original text of the component is given by an application note.

Selections filled in by the ST author appear in square brackets with an indication that a selection is 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 an application note. Assignments 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.

7.2.2 Cryptographic support (FCS)

FCS_CKM.1/ECC Cryptographic key generation - ECC

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/ECC 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, 320 bit, 384 bit, 512 bit, 521 bit that meet the following: curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18].

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. 320 bit, 384 bit, 512 bit, 521 bit

ST: assignment*: list of standards:* curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18]

FCS_CKM.4/ECC 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/ECC The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method G&D_ECDSAKeyDestr that meets the following: none.

Application note 2: The following operations have been performed:

ST: assignment*: cryptographic key destruction method:* G&D_ECDSAKeyDestr

ST: assignment*: list of standards:* none

FCS_COP.1/ECC Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm EC-DSA and cryptographic key sizes 256 bit. 320 bit, 384 bit, 512 bit, 521 bit that meet the following: curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18].

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. 320 bit, 384 bit, 512 bit, 521 bit

ST: assignment: *list of standards:* curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18]

FCS_CKM.1/RSA Cryptographic key generation - RSA

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/RSA The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm G&D_RSAKeyGen and specified cryptographic key sizes 2048 bit - 4096 bit that meet the following: [6].

Application note 4: 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_RSAKeyGen

ST: assignment*: cryptographic key sizes:* 2048 bit - 4096

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

Application note 5a: The TOE uses a propriety generation algorithm that fulfils the requirements of reference [6], for example selection of prime factors e.g.

FCS_CKM.4/RSA 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/RSA The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method G&D_RSAKeyDestr that meets the following: none.

Application note 6: The following operations have been performed:

ST: assignment*: cryptographic key destruction method:* G&D_RSAKeyDestr

ST: assignment*: list of standards:* none

FCS_COP.1/RSA Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bit - 4096 bit that meet the following: PSS and

PKCS1-v1_5 according chapter 8 and 9 of [8].

Application note 7: The following operations have been performed:

PP: assignment: *list of cryptographic operations*: digital signature creation

ST: *assignment: cryptographic algorithm:* RSA

ST: *assignment: cryptographic key sizes*: 2048 bit - 4096 bit

ST: assignment: *list of standards:* PSS and PKCS1-v1_5 according chapter 8 and 9 of [8]

7.2.3 User data protection (FDP)

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

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	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 8: No additional objects or security attributes have been defined compared to the PP.

FDP_ACC.1/SCD/SVD_Generation Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD/SVD_Generation 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 9: 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 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 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 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 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/ SCD/SVD_Generation 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 10: The following operations have been performed:

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

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 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SVD_Transfer The TSF shall enforce the SVD_Transfer SFP on
(1) subjects: S.User,
(2) objects: SVD
(3) operations: export

Application note 11: 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 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 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 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 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

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

Application note 12: The following operations have been performed:

PP: assignment: *access control SFP*: SVD_Transfer

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;

FDP_ACC.1/Signature_Creation Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Signature_Creation

The TSF shall enforce the Signature_Creation SFP on
(1) subjects: S.User,
(2) objects: DTBS/R, SCD,
(3) operations: signature creation.

Application note 13: 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 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature_Creation

The TSF shall enforce the Signature_Creation SFP 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

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

R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”.

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

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

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

Application note 14: 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.

Application note 15: 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

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":

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 16: 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 17: 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.

7.2.4 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 Chip and Terminal Authentication Protocol according to chapter 4 of [19], symmetric authentication scheme according chapter 8.8 [20], PACE according chapter 4 of [19] with AES encryption of the nonce, digital signature-generation PSS and PKCS1-v1_5 according chapter 8 and 9 of [8] and ECDSA digital signature-generation with the curves brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18] to prove the identity of the SSCD.

Application note ST: The following operations have been performed:

ST: assignment: *authentication mechanism:* Chip and Terminal Authentication Protocol according to chapter 4 of [19], symmetric authentication scheme according chapter 8.8 [20], PACE according chapter 4 of [19] with AES encryption of the nonce, digital signature-generation PSS and PKCS1-v1_5 according chapter 8 and 9 of [8] and ECDSA digital signature-generation with the curves brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according chapter 6 of [17] and the curves secp256r1, secp384r1 and secp521r1 according chapter 2 of [18]

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) establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,
(3) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/Conf_VAD,
(4) 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 18: 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:* (2)establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, (3) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/Conf_VAD, (4) 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) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/Conf_VAD,
(5) 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 19: 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) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/Conf_VAD, (5) 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 20: 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

7.2.5 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 21: 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 22: 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 23: 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 24: 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 25: 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 26: For 'SCD/SVD Management' only the secure values 'authorised' and 'not authorised' are secure for the TOE and the intended TOE lifecycle. 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 can set 'SCD / SVD Management' to 'authorised' and since authentication as Administrator is required for that, also the value 'authorised' is secure.
For 'SCD operational' only the secure values 'yes' and 'no' are accepted. SCD operational is set to 'no' as long as the RAD 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 by 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, SVD_Transfer 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 27: The following operations have been performed:
PP: assignment: *access control SFP, information flow control SFP*: SCD/SVD_Generation SFP, SVD_Transfer SFP and Signature_Creation SFP

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

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

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 28: 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.

As the TOE in the usage phase does not support generating an SVD/SCD pair by the Administrator alone, the rule (1) is not relevant in the usage phase.

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 29: 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 30: 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 31: Instead of assigning 'none' to 'other operations' the assignment has been deleted from the SFR for clarity.

7.2.6 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit information about IC power consumption, electromagnetic radiation and command execution time in excess of non useful information enabling access to RAD and SCD.

FPT_EMS.1.2 The TSF shall ensure attacker are unable to use the following interface contacts VCC, GND, IO and electromagnetic radiation to gain access to RAD and SCD.

Application note 32: 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, electromagnetic radiation and command execution time
ST: *assignment: specified limits:* non useful information
ST: *assignment: type of users:* attacker
ST: *assignment: type of connection:* contacts VCC, GND, IO and electromagnetic radiation

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 33: 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 34: 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 TSF may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1 requires the TSF to react on physical tampering in a way that the signatory is able to determine whether the TOE was physical tampered or not. E.g. the TSF may provide an appropriate message during start-up or the guidance documentation may describe a failure of TOE start-up as indication of physical tampering.

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 35: 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

7.2.7 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 FIA_API.1 and 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

Application note 36a: The TOE supports the establishment of a trusted path/channel based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity. AES 128, AES 192 and AES 256 [21] are provided by the TOE to secure the communication data according chapter 9 of [20]. Communication data can also be secured by a signature, for the supported signature mechanism and the mutual

Authentication protocols see FIA_API.1.1. As hash functions the TOE supports SHA-2 (224 bit, 256 bit, 384 bit and 512 bit) according [22].

FTP_ITC.1/Conf_VAD Inter-TSF trusted channel – TC Human Interface Device

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/ **Conf_**VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** 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/ **Conf_**VAD	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/ **Conf_**VAD	The TSF **or the HID** shall initiate communication via the trusted channel for (1) None.

Application note ST: The following operations have been performed:

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

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

ST: assignment: *list of functions for which a trusted channel is required*: None

FTP_ITC.1/Conf_DTBS Inter-TSF trusted channel – Signature creation Application

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/Conf_DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** 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/Conf_DTBS	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/Conf_DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for

(1) None.

Application note ST: The following operations have been performed:

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

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

ST: assignment: *list of functions for which a trusted channel is required*: None

7.3 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
	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

Assurance Class	**Assurance components**
	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. (FMT_SMR.1)

The Administrator can authenticate himself using Terminal Authentication Protocol according to [19], symmetric authentication scheme according [20], PACE according [19] with AES encryption of the nonce. Furthermore contactless communication requires the execution of the PACE Protocol according to [19]. 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. (FIA_AFL.1)

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. 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. (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MTD.1/Signatory)

If the TOE is issued with a generated SCD, the signatory has to first set the RAD before the SCD is operational; in the operational usage phase the RAD need to be set by the signatory before the SCD can be generated. (FMT_MSA.4)

The creation of the RAD can only be performed by the administrator during the initialisation and personalisation phase. (FMT_MTD.1/Admin)

The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication. (FIA_UID.1, FIA_UAU.1)

All security attributes under access control have secure default values and are modified in a secure way so that no unauthorised modifications are possible. (FMT_MSA.2, FMT_MSA.3)

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. (FDP_RIP.1)

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. (FDP_SDI.2/Persistent, FDP_SDI.2/DTBS)

The TOE hides information about IC power consumptions and command execution time, to ensure that no confidential information can be derived. (FPT_EMS.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. (FPT_PHP.1, FPT_PHP.3)

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. (FPT_TST.1, FPT_FLS.1)

8.4 SF_KeyManagement

The TOE contains a deterministic random number generator rated DRG.4 according to AIS20 [12]. The seed for the deterministic random number generator is provided by the PTG.2 true random number generator of the underlying IC. The TOE supports onboard generation of RSA keypairs with key length 2048 bit - 4096 bit (in 8 bit steps) and generation of ECC keypairs with key length 224 bit, 256 bit. 320 bit, 384 bit, 512 bit, 521 bit for the following curves brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according [17] and the curves secp256r1, secp384r1 and secp521r1 according [18]. (FCS_CKM.1/ECC, FCS_CKM.1/RSA)

In the case that a signature key pair is terminated on request of the signatory, the signature key pair will be deleted by the TOE. (FCS_CKM.4/ECC, FCS_CKM.4/RSA)

8.5 SF_SignatureGeneration

The TOE supports calculations with elliptic curves defined over a field F(p) with lengths of the parameters p and q of 256 bit. 320 bit, 384 bit, 512 bit, 521 bit for the following curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according [17] and the curves secp256r1, secp384r1 and secp521r1 according [18]. In addition, the TOE supports calculations of hash values according to SHA-2 (224 bit, 256 bit, 384 bit and 512 bit) according [22]. Based on these calculations the TOE supports generation of EC-DSA signatures according to chapter 6.4 of [7]. (FCS_COP.1/ECC, FIA_API.1)

Furthermore RSA calculations with key length from 2048 bit up to 4096 bit (in 8 bit steps) are supported; the signatures can be generated according PSS and PKCS1-v1_5 of chapter 8 and 9 of [8]. (FCS_COP.1/RSA, FIA_API.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. AES 128, AES 192 and AES 256 [21] are provided by the TOE to secure the communication data according chapter 9 of [20]. (FIA_API.1, FTP_ITC.1/SVD, FTP_ITC.1/Conf_VAD, FTP_ITC.1/Conf_DTBS)

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. (FDP_DAU.2/SVD)

8.7 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 7.3.

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_Auth_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_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_confTC_VAD_Imp	OT.TOE_confTC_DTBS_Imp
FCS_CKM.1/ECC	X		X	X	X										
FCS_CKM.4/ECC	X				X										
FCS_COP.1/ECC	X					X									
FCS_CKM.1/RSA	X		X	X	X										
FCS_CKM.4/RSA	X				X										
FCS_COP.1/RSA	X					X									
FDP_ACC.1/ SCD/SVD_Generation	X	X													
FDP_ACC.1/ SVD_Transfer	X												X		
FDP_ACC.1/Signature_Creation	X						X								
FDP_ACF.1/ SCD/SVD_Generation	X	X													
FDP_ACF.1/ SVD_Transfer	X												X		
FDP_ACF.1/Signature_Creation	X						X								
FDP_RIP.1					X		X								
FDP_SDI.2/Persistent				X	X	X									
FDP_SDI.2/DTBS							X	X							
FDP_DAU.2/SVD													X		
FIA_AFL.1							X								
FIA_UAU.1		X					X					X			

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_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_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_confTC_VAD_Imp	OT.TOE_confTC_DTBS_Imp
FIA_API.1												X			
FIA_UID.1		X					X								
FMT_MOF.1	X						X								
FMT_MSA.1/Admin	X	X													
FMT_MSA.1/Signatory	X						X								
FMT_MSA.2	X	X					X								
FMT_MSA.3	X	X					X								
FMT_MSA.4	X	X		X			X								
FMT_MTD.1/Admin	X						X								
FMT_MTD.1/Signatory	X						X								
FMT_SMR.1	X						X								
FMT_SMF.1	X			X			X								
FPT_EMS.1					X				X						
FPT_FLS.1					X										
FPT_PHP.1										X					
FPT_PHP.3					X						X				
FPT_TST.1	X				X	X									
FTP_ITC.1/SVD													X		
FTP_ITC.1/Conf_VAD														X	
FTP_ITC.1/Conf_DTBS															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 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and

FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_creation, FDP_ACF.1/Signature_creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD/SVD_Auth_Gen (Authorized 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 and FDP_ACF.1/SCD/SVD_Generation 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_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which 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 ensures 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 creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. The SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS 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 and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.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_EMS.1.1.

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

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

OT.TOE_SSCD_Auth (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 and FDP_ACF.1/SVD_Transfer.
- 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.

OT.TOE_confTC_VAD_Imp (Trusted channel of TOE for VAD import) is provided by FTP_ITC.1/Conf_VAD by allowing the administrator to configure the availability of a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_confTC_DTBS_Imp (Trusted channel for DTBS) is provided by FTP_ITC.1/Conf_DTBS by allowing the administrator to configure the availability of a trusted channel to protect the DTBS provided by the SCA to the TOE.

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/ECC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4/ECC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/ECC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4

Requirement	Dependencies	Fulfilled
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/RSA	[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	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/ Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/ SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/ SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/ Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/ SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FDP_RIP.1	No dependencies	n. a.
FDP_SDI.2/Persistent	No dependencies	n. a.
FDP_SDI.2/DTBS	No dependencies	n. a.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_API.1	No dependencies	n. a.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/ Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1

Requirement	Dependencies	Fulfilled
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, FDP_ACC.1/ Signature_Creation
FMT_MTD.1/ Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/ Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n. a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	No dependencies	n. a.
FPT_FLS.1	No dependencies	n. a.
FPT_PHP.1	No dependencies	n. a.
FPT_PHP.3	No dependencies	n. a.
FPT_TST.1	No dependencies	n. a.
FTP_ITC.1/SVD	No dependencies	n. a.
FTP_ITC.1/Conf_VAD	No dependencies	n. a.
FTP_ITC.1/Conf_DTBS	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 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.

9.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Infineon Chip M7820 [9]. This statement is compliant to the requirements of [13].

9.4.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functions	**Relevant**	**Not relevant**
SF_DPM: Device Phase Management	x	
SF_PS: Protection against Snooping	x	
SF_PMA: Protection against Modifying Attacks	x	
SF_PLA: Protection against Logical Attacks	x	
SF_CS: Cryptographic Support	x	

Table 5: Classification of Platform-TSFs

All listed TSFs of the Platform-ST are relevant for the Composite-ST.

9.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon Microcontroller M7820
- True Random Number Generator (TRNG) with PTG.2 classification according to AIS 31 [11]
- Cryptographic support for AES, RSA and elliptic curve calculations. For AES calculations it is assumed that they are resistant against attacks like DPA, EMA and DFA.

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

9.4.2.1 TOE Security Environment

Threats and OSPs

<u>(see chapters 4.1 and 4.2)</u>

None of the OSPs are applicable to the IC.

The following threats of this Composite-ST are directly related to IC functionality:

- T.Hack_Phys

This threat will be mapped to the following Platform-ST threats:

- T.Leak-Inherent
- T.Phys_Probing
- T.Malfunction
- T.Phys_Manipulation
- T.Leak-Forced

The following table shows the mapping of the threats.

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced
Composie-ST	T.Hack_Phys	X	X	X	X	X

Table 6: Mapping of threats

T. Hack_Phys matches to T.Leak-Inherent, T.Phys_Probing, T.Malfunction, T.Phys-Manipulation and T.Leak-Forced as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

Assumptions, see chapter 4.3:

The assumptions from this ST (A.CGA, A.SCA) make no assumption on the Platform, but to the environment of the TOE.

The assumptions from the Platform-ST are as follows:

Assumption [9]	Classification of assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC	not relevant	n/a
A.Plat-Appl	not relevant	n/a
A.Resp-Appl	relevant	All Security Objectives of this Composite TOE aim to protect the user data, especially SCD, SVD, DTBS and RAD.
A.Key-Function	relevant	OT.EMSEC_Design requires that Key-dependent functions are implemented in a way that they are not susceptible to leakage attacks.

Table 7: Mapping of assumptions

There is **no conflict** between **security environments** of this Composite-ST and the Platform-ST [9].

9.4.2.2 Security objctives

This Composite-ST has security objectives which are related to the Platform-ST.

These are:

- OT.SCD_Secrecy
- OT.Tamper_ID
- OT.Tamper_Resistance

- OT.EMSEC_Design

The following Platform-objectives could be mapped to Composite-objectives:

- O.RND
- O.Leak-Inherent
- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation

These could be mapped to the Composite-objectives as seen in the following table.

Platform-ST		O.RND	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation
Composite-ST	OT.SCD_Secrecy	X			X	
	OT.Tamper_ID			X	X	X
	OT.Tamper_Resistance			X	X	X
	OT.EMSEC_Design		X			

Table 8: Mapping of objectives

OT.SCD_Secrecy requires sufficient quality of random numbers for the generation of SCD/SVD, which matches to O.RND. Furthermore it requires correct working conditions which match to O.Malfunction.

OT.EMSEC_Design requires AES calculations without intelligible emanations within specified limits which matches to O.Leak-Inherent.

OT.Tamper_ID and OT.Tamper_Resistance require detection of and resistance to physical tampering which matches to O.Phys-Probing, O.Phys-Manipulation and O.Malfunction.

All Security Objectives for the Environment (see chapter 5.2) are not linked to the platform and are therefore not applicable to this mapping. These objectives are:

OE.SVD_Auth

OE.CGA_QCert

OE.Dev_Prov_Service

OE.DTBS_Intend

OE.Signatory

OE.CGA_SSCD_Auth

OE.CGA_TC_SVD_Imp

OE.HID_confTC_VAD_Exp

OE.SCA_confTC_DTBS_Exp

There is **no conflict** between **security objectives** of this Composite-ST and the Platform-ST [9].

9.4.2.3 Security requirements

Security Functional Requirements

This Composite-ST has the following platform related SFRs:

- FCS_CKM.1
- FIA_API.1
- FPT_EMS.1
- FPT_PHP.1
- FPT_PHP.3
- FTP_ITC.1/SVD
- FTP_ITC.1/Conf_VAD
- FTP_ITC.1/Conf_DTBS
- FPT_TST.1

The following Platform-SFRs could be mapped to Composite-SFRs:

- FCS_RNG.1
- FCS_COP.1/AES
- FDP_ITT.1
- FPT_ITT.1
- FDP_IFC.1
- FRU_FLT.2
- FPT_FLS.1
- FPT_PHP.3
- FPT_TST.3

They will be mapped as seen in the following table.

Platform-ST		FCS_RND.1	FDP_ITT.1	FPT_ITT.1	FDP_IFC.1	FCS_COP.1/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FPT_TST.2
Composite-ST	FCS_CKM.1	X								
	FIA_API.1					X				
	FPT_EMS.1		X	X	X					
	FPT_PHP.1						X	X	X	
	FPT_PHP.3						X	X	X	
	FPT_TST.1									X
	FTP_ITC.1/SVD					X				
	FTP_ITC.1/Conf_VAD					X				
	FTP_ITC.1/Conf_DTBS					X				

Table 9: Mapping of SFRs

FCS_CKM.1 requires sufficient quality of random numbers for the generation of SCD/SVD, which matches to FCS_RND.1.

FPT_EMS.1 require the prevention of disclosure of secret data while being processed which is provided by FPT_ITT.1, FDP_ITT.1 and FDP_IFC.1.

FTP_ITC.1/SVD, FTP_ITC.1/Conf_VAD, FTP_ITC.1/Conf_DTBS and FIA_API.1 require cryptographic calculations which match to FCS_COP.1/AES.

FPT_PHP.1 and FPT_PHP.3 of the composite ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the platform ST.

FPT_TST.1 run a suite of self tests to demonstrate the correct operation of the TSF which matches to FPT.TST.2.

Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R3 augmented by AVA_VAN.5

The Platform-ST requires EAL 5 according to Common Criteria V3.1 R3 augmented by:

ALC_DVS.2, AVA_VAN5

As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of the Composite-ST will match to the Platform-ST assurance requirements. But also the augmented parts of the Composite-ST match to the Platform-ST.

9.4.3 Overall no contracdictions found

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

10 Acronyms

CC	Common Criteria
CGA	Certification generation application
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
(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.

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**: 2.2) means an digital 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.

Annex references one of the annexes, Annex I, Annex II or Annex III of **The Directive**

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

Certificate means an electronic attestation, which links the SVD to a person and confirms the identity of that person (**The Directive:** 2. 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 with an identifier of the hash function used to compute the hash values.

Certificate info may contain information to allow the user to distinguish between several certificates.

Certification generation application (**CGA**) means a collection of application elements which receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate.

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

Common Criteria (CC) is set of rules and procedures for evaluating the security properties of a product

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.

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

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

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

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

Qualified electronic signature means an advanced signature that has been created with an SSCD with a key with a qualified certificate (c.f. **The Directive: 5.1**).

Reference authentication data (RAD) means data persistently stored by the TOE to authenticate a user as authorised for a particular role.

SSCD-provisioning service is a 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 Directive:** 2.5 and 2.6).

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

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

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

Signature creation application (SCA) means the application complementing an SSCD with a user interface with the purpose to create an electronic signature.

Note: A signature creation application is software consisting of a collection of application components configured to:

• present the data to be signed (DTBS) for review by the signatory,

• obtain prior to the signature process a decision by the signatory,

• if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE

• process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

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

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) is the public cryptographic key that can be used to verify an electronic signature (**The Directive**: 2.7).

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.

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

The Directive references Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on "*a Community framework for electronic signatures*"[10]

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

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

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

Verification authentication data (VAD) means authentication data provided as input to a secure signature creation device for authentication by cognition.

[10] References in this document to a specific article and paragraph of Directive 1999/93/ec are of the form, (**The Directive**: n.m)".

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 4 Final, CCMB-2012-09-001, September 2012

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

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

[5] Protection profiles for Secure signature creation device – Part 2: Device with key generation, prEN 14169-2:2012; Version 2.0.1; 2012-01, BSI-CC-PP-0059-2009-MA-01

[5a] Protection profiles for Secure signature creation device – Part 2: Device with key generation; prEN 14169-2:2010; Version 1.8; 2011-04

[6] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) Vom 30. Dezember 2011; Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243

[7] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2006

[8] PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002

[9] Security Target, Infineon, M7820 A11 and M11, Version 1.5, 07.05.2012.

[10] Protection Profile –Security IC Platform, version 1.0, 15.06.2007, BSI-CC-PP-0035

[11], [12] Evaluation of random number generators, Version 0.8, BSI, 9.12.2011

[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 for Secure Signature Creation Device - Part 1: Overview; prEN 14169-1:2010; 2010-01

[15] Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application; prEN 14169-4:2010; Version 0.8

[16] Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature creation application; prEN 14169-5:2010; Version 0.8

[17] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000, Version 1. http://www.secg.org/collateral/sec2_final.pdf

[19] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), TR-03110, Version 2.05, 14.10.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] EN 14890-1:2008 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

[21] NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197, 2001

[22] NIST. Secure hash standard (and Change Notice to include SHA-224), FIPS PUB 180-2, 2002