ASEPCOS-CNS/CIE Public Security Target

ASEPCOS-CNS/CIE with Digital Signature Application
on Atmel AT90SC144144CT

SSCD-PP Type 3 compliant
Version 1.05, EAL4+, CWA 14169:2002 E

Version 1.0
17 Oct. 07

Athena Smartcard Solutions, Inc.

Contents

List of Tables

List of Figures

1. ST introduction

1.1. ST identification

ST title:	**ASEPcos-CNS/CIE with Digital Signature Application on Atmel AT90SC144144CT Security Target**
Authors:	Athena Smartcard Solutions
General Status:	Final version for certification
Public ST version:	1.0
ST Version:	2.4
Date of production:	11 October 2007
TOE:	ASEPCOS CNS/CIE Version 1.60 Build 001 AT90SC144144CT Product Identification Number: AT58807 Revision: G Atmel Toolbox Version: 00.03.01.04
CC Version:	2.3 Final of August 2005 - Part 1: CCMB 2005-08-001 - Part 2: CCMB 2005-08-002 - Part 3: CCMB 2005-08-003
PP Claim:	Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Represented CWA: CWA 14169:2002 E (annex A) PP Identification PP0006b Report Identification: PP0006a

ASEPCOS-CNS/CIE is embedded on Atmel AT90SC144144CT smart card IC evaluated to CC EAL4+ according to PP9806 [9] and ST [11] as reported in the Certificate Report [10].

1.2. ST overview

This ST describes the security functions of the ASEPCOS with EU compliant Digital Signature Application 'CNS/CIE' (Hereinafter referred to as the TOE). This configuration of ASEPCOS enforces the security functions required for digital signature and supports usage only through secure trusted communication channels. The TOE implements a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [1] as a smart card which allows the generation of signature creation data (SCD) and the creation of qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized Signatory can use it.

ASEPCOS is a multi-application ISO7816 compatible smart card OS which supports RSA cryptography of up to 2048 RSA.

The underlying hardware platform on which the ASEPCOS software is implemented is the Atmel AT90SC144144CT IC supporting contact interface. This IC is certified according to CC EAL 4+ [10]

and its Security Target is compliant with PP9806 [9].

The TOE meets all the following requirements as defined in the European Directive (article 2.2):

(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

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

The TOE consists of the software and hardware parts.

1.3. CC conformance

The ST is conformant to CC Version 2.3 Part 2 [1] (with extension made in SSCD PP [6]) and CC Version 2.3 Part 3 [2].

The ST claims conformance to SSCD Type 3 Protection Profile [6]

The assurance level for this ST is EAL4 augmented with: AVA_MSU.3 and AVA_VLA.4

The minimum strength level for the TOE security functions is ‘SOF High’ (Strength of Functions High).

2. TOE Description

2.1. General

The TOE is a smart card IC where digital application software is stored in NVM.

The TOE is linked to a card reader/writer via the HW and physical interfaces of the smartcard. The smartcard has only contact type interfaces and may be applied to the contact type card reader/writer. The card reader/writer is connected to a computer such as a personal computer and allows Application Programs (APs) to use the TOE. The contact type interface of the smartcard is ISO/IEC 7816 compliant.

There are no other external interfaces of the smartcard except ones described above. Figure 2-1 shows the boundaries of the TOE within the smart card.

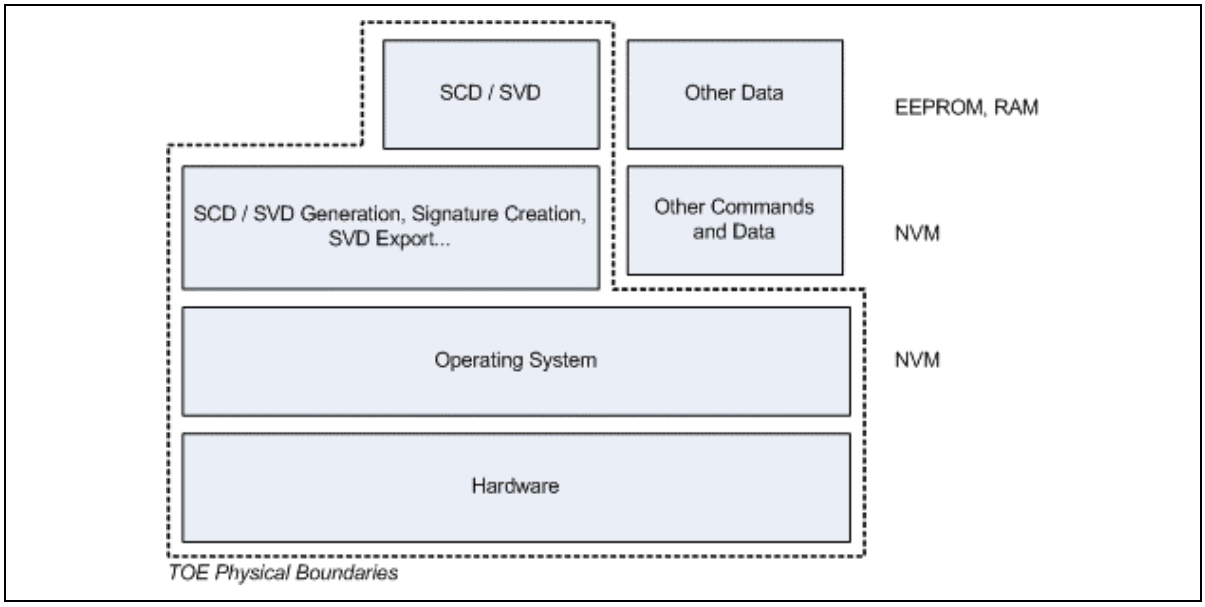


Figure 1 - TOE Description

2.2. Secure Signature Creation Devices

The following is an introduction to SSCD based on the SSCD Protection Profile [6].

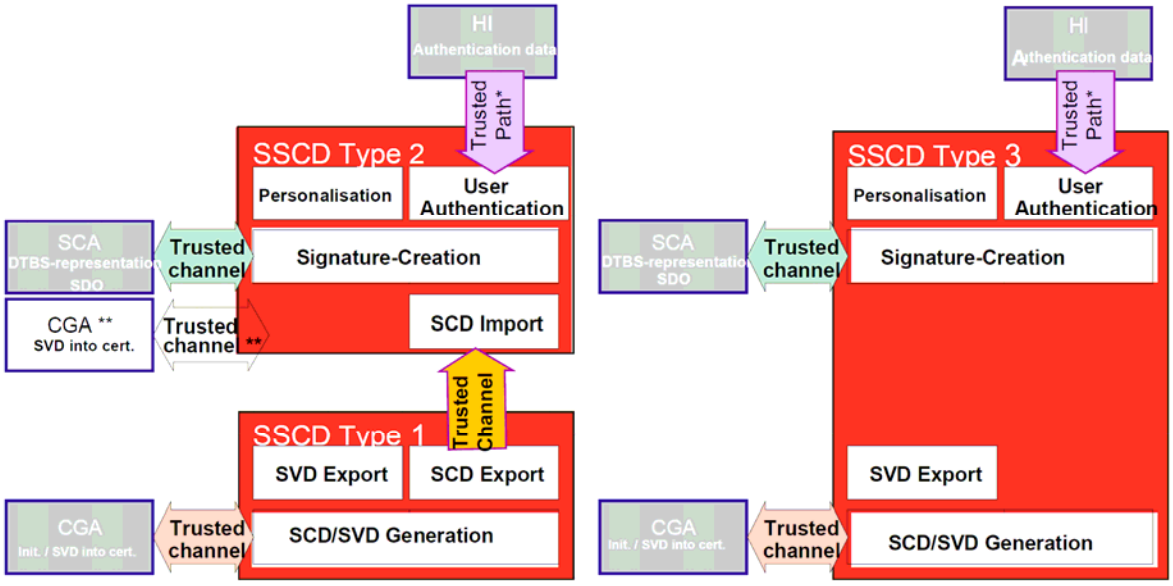
The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as ‘SSCD types’, as illustrated in Figure 2-2.

If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation (“Init.”) and the SSCD exports the SVD for generation of the corresponding certificate (“SVD into cert.”).

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 3 (e.g., a smart card).The Human Interface (HI) for such signatory authentication is not provided by the SSCD, and thus a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel.

The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 3 components are personalized components: they can be used for signature creation by one specific user – the signatory - only.



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)

Figure 2 - SSCD types and modes of operation

2.3. Limits of the TOE

The TOE is a secure signature-creation device (SSCD type3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD.

The TOE described in this ST is a smart card operating system implemented on a smart card IC which is certified CC EAL 4+. The TOE includes embeddable software in the NVM of the IC and a file system including the digital signature application stored in EEPROM. Parts of the operating systems may be stored in EEPROM.

NVM (Non Volatile Memory) corresponds to FLASH memory for the Atmel AT90SC144144CT IC

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

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

(2) to create qualified electronic signatures

- (a) after allowing for the data to be signed (DTBS) to be displayed correctly by the appropriate environment
- (b) using appropriate hash functions that are, according to [5], agreed as suitable for qualified electronic signatures
- (c) after appropriate authentication of the signatory by the TOE
- (d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [5]

The TOE implements functions to ensure the secrecy of the SCD. To prevent the unauthorized usage of the SCD, the TOE provides user authentication and access control. The TOE user is authenticated by presenting a VAD which is verified against the RAD which is stored securely in the TOE. The TOE also provides measures to support a trusted paths and/or channels. The SCA which is used to present the data to be signed is not implemented by the TOE and is considered as part of the environment of the TOE.

The SSCD protects the SCD during the whole life cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE will be initialized for the signatory's use by

(1) generation of SCD/SVD pair

(2) personalisation for the signatory by means of the signatory's verification authentication data (SVAD)

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

Figure 2 shows the PP scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

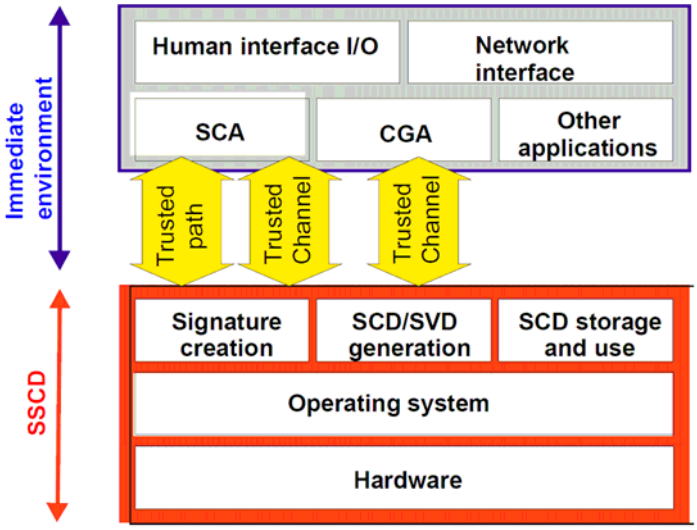


Figure 3 - Scope of the SSCD, structural view

The smart card HW and Software in which the SSCD application is installed can contain additional functions and files which are not related to the digital signature application and do not influence it or interact with it in any way and are regarded as data structures. Such applications and files are beyond the scope of this TOE.

2.4. TOE life cycle

The TOE life cycle is shown in Figure 3. Basically, it consists of a development phase and the operational phase.

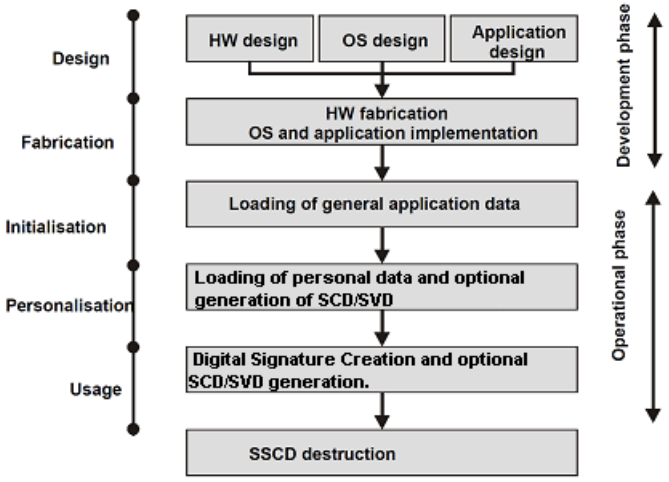


Figure 4 - SSCD life cycle

2.4.1. Development Phase

HW Design – Atmel

OS Design – Athena Development department

Application Design – Athena Development department

HW Fabrication and OS & Application implementation – Atmel

The operating system part of the TOE which is developed by Athena is sent in a secure way to Atmel for masking in NVM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip.

Initialization may be done in parts at various facilities and personalization can be done by Athena, 3rd Party initialization facility or Card Issuer/Customer. The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.

This ST addresses the functions used in phases 4 to 7 but developed during development phase.

2.4.2. Operational Phase

Initialization – Athena or 3rd Party initialization facility/Card Manufacturer which includes loading of the General Application Data

Personalization – Athena or 3rd Party Personalization facility which includes the optional generation of the SCD/SVD pair and loading of Personal Application Data

Usage – Where upon the card is delivered from the Customer (the Card Issuer) to the End User and the End User may use it for signature-creation including all supporting functionality (e.g., SCD storage and SCD use) but only following a correct verification of the initial PIN-Activate PIN which allows the End User to make sure that he is the first user to ever use this SCA for digital signature.

2.4.3. Application note: Scope of SSCD PP application

This ST refers to qualified certificates as electronic attestation of the SVD corresponding to the signatory's SCD that is implemented by the TOE.

While the main application scenario of a SSCD will assume a qualified certificate to be used in combination with a SSCD, there still is a large benefit in the security when such SSCD is applied in other areas and such application is encouraged. The SSCD may as well be applied to environments where the certificates expressed as 'qualified certificates' in the SSCD do not fulfil the requirements laid down in Annex I and Annex II of the Directive [1].

When an instance of a SSCD is used with a qualified certificate, such use is from the technical point of view eligible for an electronic signature as referred to in Directive [1], article 5, paragraph 1. This Directive does not prevent TOE itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

2.5. Features of the ASEPCOS-CNS/CIE – Informational

This section is information and intended to provide general details about the ASEPCOS-CNS/CIE OS which implements the TOE. Information in this section does not extend the TOE description or claims of this ST.

ASEPCOS is a general purpose multi-application cryptographic smart card operating system supporting JICSAP 2.0, CNS, and ICAO LDS.

ASEPCOS complies with ISO 7816.

ASEPCOS-CNS/CIE is designed to comply with the Italian CNS specifications, Italian digital signature law and European electronic signature directive.

The API exposed by ASEPCOS allows for fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and payment applications.

2.5.1. File System

Directory structure depth up to 8 levels
Maximum number of active authentication keys – 256
DF can have DF Name and/or DF-ID
Record files can have Binary or TLV records
Records can be accessed using current record pointer and tag value, in addition to record number

2.5.2. Features

ASEPCOS is designed for the Atmel AVR family of smart card microprocessors and specifically the Atmel AT90SC144144CT IC supporting contact interface and is certified according to the CC EAL 4+ [10]. ASEPCOS is protected against state of the art attacks.

The OS:

- supports ISO 7816-4, 8 and 9 standards and PC/SC applications
- provides fast cryptography
- enforces smart memory management
- provides strong security and data integrity mechanisms
- has been designed with PKI in mind

2.5.3. Secure Messaging

All commands can be secured

ASEPCOS-CNS/CIE supports both CNS and ICAO Secure Messaging schemes (static keys and session keys)

Supports extended length APDUs with data length up to 64K bytes (ICAO mode).

2.5.4. Keys and security

ASEPCOS-CNS/CIE provides up to 256 authentication keys (or PINS) under secure conditions.

Private RSA keys that are generated from internal random source are tagged. Application can differentiate between keys that have never left the card and keys that were imported from outside.

All keys have attributes that can help detect and prevent unauthorized usage and change of keys. Authentication keys may have the AutoClear attribute. When such a key is used, the corresponding bit in the security status is automatically cleared.

Security Status protects application's data from being accessed by other applications.

All DES keys are checked against "weak key" values.

2.5.5. Memory Management

All internal file system structures in non-volatile memory are updated using "atomic operations". This provides safe operations even when power is interrupted.

Key data integrity is verified using CRC16 each time before a key is used.

Deleted files are erased and returned to the "free memory pool" for reuse.

DF can optionally have a "size quota" (pre-allocated fixed memory area). Otherwise, a DF can expand dynamically to the full memory capacity of the card.

2.5.6. Cryptography

Counter measures against state of the art attacks such as SPA/DPA.

FIPS compatible Random Number Generator algorithm (using hardware generated seed as input to SHA1).

RSA signature calculation and verification according to PKCS#1 standard [13] (1024 to 2048 bits).

SHA1 and RIPEMD160 hash algorithms (ISO 7816-8 compatible).

3DES encryption and decryption (16 or 24 bytes, ECB and CBC modes)

3DES Message Authentication Code (16 or 24 bytes, MAC).

Key Pair generation (RSA).

2.5.7. Performance

ASEPCOS-CNS/CIE supports T=1 protocol (T=0 is optional), with speeds of up to 115200 baud.

Fast RSA Key Generation

Fast implementation of Rabin-Miller prime-number test algorithm. The number of iterations can be changed to any number between 3 and 15 (default is 4).

Optional private key generation based on strong primes.

Fast RSA Signature Calculation

All RSA private key operations (Signature Calculation, Internal Authentication, Decrypt) use the Chinese Remainder Theorem, resulting in faster operations (this includes RSA private keys that are imported as <d, n>).

3. TOE security environment

3.1. Assets

1. **SCD**: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

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

3. **DTBS** and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

4. **VAD**: PIN, PUK, Activate-PIN code or biometrics data entered by the End User to perform a signature operation, changing and unblocking (confidentiality and authenticity of the VAD as needed by the authentication method employed)

5. **RAD**: Reference PIN, PUK, Activate-PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)

6. **Signature-creation function** of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures)

7. **Electronic signature**: (Unforgeability of electronic signatures must be assured).

Note: *Biometrics is no supported by the TOE and thus Biometric Data and Authentication Reference assets, as presented in the SSCD type 3 PP, are not included.*

3.2. Subjects

Subjects	Definition
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

3.3. Threat agents

S.OFFCARD	Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a **high level potential attack** and **knows no secret.**

3.4. Assumptions

A.CGA *Trustworthy certification-generation application*

The CGA protects the authenticity of the signatory's name 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-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

3.5. Threats to Security

T.Hack_Phys *Physical attacks through the TOE interfaces*

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

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

An atacker can store, copy, the SCD outside the TOE. An attacker can release 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 public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery *Forgery of the electronic signature*

An attacker forges the signed data object maybe together with its electronic signature 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 generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud *Repudiation of signatures*

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. This results in the signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery *Forgery of the signature-verification data*

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

T.DTBS_Forgery *Forgery of the DTBS-representation*

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.

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.SOFT_ARCHI *Corruption of software and IC designer information*

An attacker could corrupt the program and data if the smartcard embedded software is not developed in a secure manner, that is focusing on their integrity.

T.DEV_ORG *Corruption of software*

An attacker could corrupt Smart Card Embedded Software (e.g. program and any data) used during the development phase. Such qttqck could be done if the procedures dealing with physical, personnel, organizational, technical measures for the integrity can be violated (do not exist or are not applied) during the application design phase.

3.6. Organisational Security Policies

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alias the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign *Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (according to directive Annex 1) and is created by a SSCD.

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

The TOE implements the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

4. 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 organizational security policies and assumptions.

OT.SCD_SVD_Corresp has been modified between the PP and this document as there is no on-demand correspondence verification for the SCD/SVD. The reason being that the SCD/SVD are not imported in the TOE but generated by the TOE.

4.1. Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-generation.

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

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

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify the correspondence between the SCD and the SVD when they are generated by the TOE on demand.

OT.SVD_Auth_TOE *TOE ensures authenticity of the SVD*

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

OT.Init *SCD/SVD generation*

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.

OT.Tamper_ID *Tamper detection*

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance *Tamper resistance*

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

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

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible low.

OT.DTBS_Integrity_TOE *Verification of the DTBS-representation integrity*

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS-representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

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

The TOE provides the signature generation 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.Sig_Secure *Cryptographic security of the electronic signature*

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

4.2. Security Objectives for the Environment

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA *CGA verifies the authenticity of the SVD*

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.HI_VAD *Protection of the VAD*

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.SOFT_DLV *Secure Software Delivery*

The smartcard embedded software must be delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.

OE.SCA_Data_Intend *Data intended to be signed*

The SCA

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

OE.DEV_TOOLS *Secure Software design*

The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc...) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.

OE.SOFT_MECH *Software mechanisms activation*

The smartcard embedded software shall use IC security features and security mechanisms as specified in the Smartcard IC documentation (e.g. sensors...).

5. IT Security Requirements

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

Security functional requirements components given in section 5.1 “TOE security functional requirements”, except FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3].

Operations for assignment, selection and refinement have been made and are designated by an underline (e.g. none), in addition, where operations that were uncompleted in the PP [6] are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

5.1. TOE Security Functional Requirements

5.1.1. Cryptographic support (FCS)

5.1.1.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *between 1024 bit and 2048 bit* that meet the following: *Algorithms and parameters for algorithms [5].*

5.1.1.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method *overwriting old key with new key* that meets the following: *none*.

Application notes:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

5.1.1.3. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *between 1024 bit and 2048 bit* that meet the following: *Algorithms and parameters for algorithms* [*5*].
FCS_COP.1.1/ SIGNING	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *between 1024 bit and 2048 bit* that meet the following: *Algorithms and parameters for algorithms* [*5*].

5.1.2. User data protection (FDP)

5.1.2.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SVD TRANSFER SFP	The TSF shall enforce the SVD Transfer SFP on export of SVD by User.
FDP_ACC.1.1/ INITIALISATION SFP	The TSF shall enforce the Initialization SFP on generation of SCD/SVD pair by User.
FDP_ACC.1.1/ PERSONALISATION SFP	The TSF shall enforce the Personalization SFP on creation of RAD by Administrator.
FDP_ACC.1.1/ SIGNATURE CREATION SFP	The TSF shall enforce the Signature-creation SFP on 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory.

5.1.2.2. Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
Initialization attribute		
User	SCD / SVD management	authorized, not authorized
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorized SCA	no, yes

Initialization SFP

FDP_ACF.1.1/ INITIALISATION SFP	The TSF shall enforce the Initialisation SFP to objects based on the following: General attribute and Initialisation attribute.
FDP_ACF.1.2/	The TSF shall enforce the following rules to determine if an operation

INITIALISATION SFP	among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “authorised” is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/ INITIALISATION SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ INITIALISATION SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: The user with the security attribute “role” set to “Administrator” or set to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair.

SVD Transfer SFP

FDP_ACF.1.1/ SVD TRANSFER SFP	The TSF shall enforce the SVD Transfer SFP to objects based on the following: General attribute.
FDP_ACF.1.2/ SVD TRANSFER SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “Administrator” or to “Signatory” is allowed to export SVD.
FDP_ACF.1.3/ SVD TRANSFER SFP	The TSF shall explicitly authorise access of subjects to objects based On the following additional rules: none.
FDP_ACF.1.4/ SVD TRANSFER SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none.

Personalisation SFP

FDP_ACF.1.1/ PERSONALISATION SFP	The TSF shall enforce the Personalisation SFP to objects based on the following: General attribute.
FDP_ACF.1.2/ PERSONALISATION SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Administrator” is allowed to create the RAD.
FDP_ACF.1.3/ PERSONALISATION SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ PERSONALISATION SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: none

Signature-creation SFP

FDP_ACF.1.1/ SIGNATURE CREATION SFP	The TSF shall enforce the Signature-creation SFP to objects based on the following: General attribute and Signature-creation attribute group.
FDP_ACF.1.2/ SIGNATURE CREATION SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Signatory” is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the

Signatory which security attribute “SCD operational” is set to “yes”.

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

FDP_ACF.1.4/ SIGNATURE CREATION SFP — The TSF shall explicitly deny access of subjects to objects based on the rules:

(a) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS which is not sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”.

(b) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “no”.

5.1.2.3. Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1/ SVD TRANSFER — The TSF shall enforce the SVD Transfer when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2/ SVD TRANSFER — The TSF shall export the user data without the user data's associated security attributes.

5.1.2.4. Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1/DTBS — The TSF shall enforce the Signature-creation SFP when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/DTBS — The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/DTBS — The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: DTBS-representation shall be sent by an authorised SCA.

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

5.1.2.5. Subset residual information protection (FDP_RIP.1)

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, VAD, RAD.

5.1.2.6. Stored data integrity monitoring and action (FDP_SDI.2)

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

1. SCD
2. RAD
3. SVD (if persistent stored by TOE).

FDP_SDI.2.1/ PERSISTANT — The TSF shall monitor user data stored within the TSC for integrity error on all objects, based on the following attributes: *data integrity redundancy code*.

FDP_SDI.2.2/ PERSISTANT — Upon detection of a data integrity error, the TSF shall
1. prohibit the use of the altered data
2. inform the Signatory about integrity error.

The DTBS-representation temporarily stored by TOE has the user data attribute "integrity checked stored data":

FDP_SDI.2.1/DTBS — The TSF shall monitor user data stored within the TSC for integrity error on all objects, based on the following attributes: integrity checked stored data.

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 Signatory about integrity error.

5.1.2.7. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD TRANSFER — The TSF shall enforce the SVD Transfer SFP to be able to transmit user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/ SVD TRANSFER — The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

FDP_UIT.1.1/ TOE DTBS — The TSF shall enforce the Signature-creation SFP to be able to receive the DTBS-representation in a manner protected from modification, deletion and insertion errors.

FDP_UIT.1.2/ TOE DTBS — The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

5.1.3. Identification and authentication (FIA)

5.1.3.1. Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 — The TSF shall detect when *a certain number of* unsuccessful authentication attempts occur related to: *RAD authentication (3 attempts are allowed) and PUK authentication (10 attempts are allowed)*.

FIA_AFL.1.2 — When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall block RAD.

5.1.3.2. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 — The TSF shall maintain the following list of security attributes belonging to individual users: RAD.

5.1.3.3. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 — The TSF shall allow
1. Identification of the user by means of TSF required by FIA_UID.1.
2. Establishing a trusted path between local user and the TOE by

means of TSF required by FTP_TRP.1/TOE.

3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.

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:

"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

5.1.3.4. Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
2. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.

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.

5.1.4. Security management (FMT)

5.1.4.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to enable the functions signature-creation function to Signatory.

5.1.4.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/ ADMINISTRATOR The TSF shall enforce the Initialisation SFP to restrict the ability to modify the security attributes SCD /SVD management to Administrator.

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 Signatory.

5.1.4.3. Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.4.4. Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the Initialisation SFP and Signature-creation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

Refinement: The security attribute of the SCD "SCD operational" is set to "no" after generation of the SCD.

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

5.1.4.5. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to modify *or unblock* the RAD to Signatory.

5.1.4.6. Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *Creation of RAD, Modifying of RAD, Access Condition Management*.

5.1.4.7. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles Administrator and Signatory.

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

5.1.5. Protection of the TSF (FPT)

5.1.5.1. Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2. TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information of IC Power consumption* in excess of *State of the Art values* enabling access to RAD and SCD.

FPT_EMSEC.1.2 The TSF shall ensure *S.OFFCARD* is unable to use the following interface *physical chip contacts* to gain access to RAD and SCD.

Application note:

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.

5.1.5.3. Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *Random Number Generation failure, EEPROM failure, out of range temperature, clock and voltage of chip*.

5.1.5.4. Passive detection of physical attack (FPT_PHP.1)

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.

5.1.5.5. Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *Physical Intrusions* to the *IC Hardware* by responding automatically such that the TSP is not violated.

5.1.5.6. TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up or before running a secure operation* 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.

5.1.6. Trusted path/channels (FTP)

5.1.6.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD TRANSFER The TSF shall provide a communication channel between itself and a remote 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 TRANSFER The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD TRANSFER The TSF **or the CGA** shall initiate communication via the trusted channel for export SVD.

FTP_ITC.1.1/ DTBS IMPORT The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ DTBS IMPORT The TSF shall permit the **SCA** to initiate communication via the trusted channel.

FTP_ITC.1.3/ DTBS IMPORT The TSF **or the SCA** shall initiate communication via the trusted channel for signing DTBS-representation.

5.1.6.2. Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

FTP_TRP.1.1/TOE The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2/TOE The TSF shall permit *local users* to initiate communication via the trusted path.

FTP_TRP.1.3/TOE The TSF shall require the use of the trusted path for *initial user authentication.*

Refinement:

The local and initial user who can communicate and authenticate with the TOE via a trusted path is the Signatory only.

5.2. TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 5.2 of SSCD PP [6].

Table 1 - Assurance Requirements: EAL(4) augmented with AVA_MSU.3 and AVA_VLA.4

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4

5.3. Security Requirements for the IT Environment

5.3.1. Certification generation application (CGA)

5.3.1.1. Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA — The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: *none*.

5.3.1.2. Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA — The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: *none*.

5.3.1.3. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SVD IMPORT — The TSF shall enforce the SVD import SFP to be able to receive user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/ SVD IMPORT — The TSF shall be able to determine on receipt of user data, whether modification and insertion has occurred.

5.3.1.4. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SVD IMPORT — The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ SVD IMPORT — The TSF shall permit *TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD IMPORT — The TSF **or the TOE** shall initiate communication via the trusted channel for import SVD.

5.3.2. Signature creation application (SCA)

5.3.2.1. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA HASH — The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm *SHA-1 or RIPEMD-160* and cryptographic key sizes none that meet the following: [***5***]

5.3.2.2. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ SCA DTBS — The TSF shall enforce the Signature-creation SFP to be able to transmit user data in a manner protected from modification, deletion and insertion errors.

FDP_UIT.1.2/ SCA DTBS — The TSF shall I be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

5.3.2.3. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ SCA DTBS	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCA DTBS	The TSF shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCA DTBS	The TSF **or the TOE** shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD.

5.3.2.4. Trusted path (FTP_TRP.1)

The trusted path between the TOE and the SCA will be required only if the human interface for user authentication is not provided by the TOE itself but by the SCA.

FTP_TRP.1.1/ SCA	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ SCA	The TSF shall permit *local users* to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path *for: initial user authentication, modification of RAD***.**

5.4. Security Requirements for the Non-IT Environment

R.Administrator_Guide *Application of Administrator Guidance*

The implementation of the requirements of the Directive, ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE.

Appropriate supervision of the CSP or other relevant entities shall ensure the ongoing compliance.

R.Sigy_Guide *Application of User Guidance*

The SCP implementation of the requirements of the Directive, ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (k), stipulates the signatory to follow the user guidance provided for the TOE.

R.Sigy_Name *Signatory’s name in the Qualified Certificate*

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive [1], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

6. TOE summary specification

6.1. TOE Security Functions

Description of TOE Security Functions:

- SF.Access Control
- SF.Identification and Authentication
- SF.Signature Creation
- SF.Secure Messaging
- SF.Crypto
- SF.Protection

6.1.1. SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1)and data communication required are satisfied. The function includes:

Control over the authorization of Users (Administrator and Signatory) to generate the SCD/SVD key pair.

Control over the management of the SCD/SVD security attributes provided only to the Administrator (SCD/SVD Management) and after the key pair is generated, the “SCD/SVD management” is set to “not authorized” by the Administrator (FDP_ACC.1/INITIALISATION SFP, FDP_ACF.1/INITIALISATION SFP, FMT_MSA.1/ADMINISTRATOR, FMT_SMF.1).

Control over the setting of the security attribute “SCD Operational” provided only to the Administrator. The Administrator sets the security attribute “SCD Operational” to “No” following the initial generation of the SCD/SVD pair (FMT_MSA.3)

Control over the Users allowed to export SVD and enforcement of secure messaging (FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP).

(FDP_ACC.1/INITIALISATION SFP, FDP_ACF.1/INITIALISATION SFP, FMT_MSA.1/ADMINISTRATOR, FMT_SMF.1).

Creation of the RAD is authorized only for Administrator during personalization.

Signatory alone is allowed to sign DTBS data and the DTBS is send by an authorized SCA (FDP_ACC.1/ SIGNATURE CREATION SFP, FDP_ACF.1/ SIGNATURE CREATION SFP, FMT_MOF.1). Any security attributes associated with the DTBS are ignored.

Signatory alone is allowed to activate the SCD and set its operational state to “Yes” (FMT_MSA.1/Signatory, FMT_SMF.1)

Signatory alone is allowed to unblock and modify the RAD (FMT_MTD.1, FMT_SMF.1_).

FDP_ACC.1/SVD TRANSFER SFP, FDP_ACC.1/INITIALISATION SFP, FDP_ACC.1/SIGNATURE CREATION SFP, FDP_ACF.1/INITIALISATION SFP, FDP_ACF.1/SIGNATURE CREATION SFP, FDP_ITC.1/DTBS, FMT_MOF.1, FMT_MSA.1/ADMINISTRATOR, FMT_MSA.1/SIGNATORY, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.1.2. SF.Identification and Authentication

This TSF manages the identification and authentication of the Signatory and Administrator and enforces role separation (FMT_SMR.1)

The Administrator is identified through the relevant access rights during the initialization and personalization of the TOE.

The authentication of the Signatory is made through presentation of the VAD and comparison with the stored RAD with a minimum length of 6 digits (FIA_ATD.1) and maximum attempts of 3 for the PIN, 3 for the Activate PIN and 10 for the PUK. Changing of the RAD requires the correct entry of the PUK.

The Signature Creation Function is made operational by the Signatory entering an initial PIN – Activate-PIN. Validating the Activate-PIN can only be performed once.

The Signatory is identified as such following the Signature Creation Function activation. Authentication of the Signatory is through presentation of the correct RAD to the TOE (FIA_UAU.1).

TSF mediated actions cannot are not allowed by the TOE before the user is identified (FIA_UID.1) authenticated and associated to the role of Signatory and if required a trusted path was established (FDP_ACC.1/SVD TRANSFER SFP)

If the verification of the VAD against the RAD fails, the TOE will register the failure by updating the retry counter of the RAD. When the retry counter is 0, the RAD will be blocked (FIA_AFL.1).

Following satisfaction of the appropriate security attributes, the RAD can be unblocked and the reset counter is returned to the initial value (FMT_MTD.1.1).

Following the satisfaction of the appropriate security attributes, the RAD can be modified by the Signatory (FMT_MTD.1.1).

Initial creation of the RAD is restricted to the Administrator (FDP_ACC.1/PERSONALISATION SFP, FDP_ACF.1/PERSONALISATION SFP, FMT_SMF.1)

IC power variation emanation is below state of the art values, and physical access to the RAD is protected during this SF activity (FPT_EMSEC.1).

The strength of this function is SOF High.

FDP_ACC.1/SVD TRANSFER SFP, FDP_ACC.1/PERSONALISATION SFP, FDP_ACF.1/PERSONALISATION SFP, FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FMT_MTD.1.1, FMT_SMF.1, FMT_SMR.1, FPT_EMSEC.1

6.1.3. SF.Signature Creation

This TSF is responsible for signing DTBS data using the SCD by the Signatory, following successful authentication of the Signatory.

The SF generates digital signatures using RSA 1024 to 2048 bit (FMT_MSA.2, FCS_COP.1) and SHA-1 or RIPEMD-160 hashing calculated by SF.Crypto. The signature is calculated based on PKCS#1 version 1.5 [13].

A hash value calculated over the DTBS is sent to the TOE by the IT Environment.

The integrity of the hash value is maintained through the use of SF. Secure Messaging.

IC power variation emanation is limited to below state of the art values, and physical access to the SCD is protected during this SF activity (FPT_EMSEC.1).

FCS_COP.1, FMT_MSA.2, FPT_EMSEC.1

6.1.4. SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.

Various data and processes such as DTBSs, signatures, public keys, identification and authentication data, SVD Transfer or other user data are embedded in command and response frames. The SF.Secure Messaging function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device. The secure communication channels are supported with cryptographic functions and provide for 3 distinct channels (TOE to CGA, TOE and SCA, TOE and User) logically distinct from each other and other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

During SVD export (FTP_ITC.1/SVD Transfer) and SVD import (FDP_UIT.1/SVD Transfer), a communication channel between the TOE and the CGA is established with secure messaging. Secure messaging also maintains the integrity of the exported and imported SVD. The SVD is exported without associated security attributes.

During import of the DTBS from the SCA to the TOE, a trusted channel, through secure messaging, is established between the SCA and the TOE (FTP_ITC.1/DTBS import, FDP_UIT.1/TOE DTBS). Secure Messaging maintains the integrity of the DTBS during import.

The CGA, SCA and local user are allowed to initiate the communication with the TOE through via a trusted channel (FTP_ITC.1/SVD Transfer, FTP_ITC.1/DTBS import, FTP_TRP.1/TOE)

During the change of RAD secure messaging is enforced (FMT_SMF.1)

This function is responsible for confidentiality and data authentication.

Confidentiality is ensured through the encryption of communication data by symmetric cryptography by the use 3DES operations. Data authentication and integrity is achieved by calculating of a cryptographic checksum (MAC).

FDP_ACC.1/SVD TRANSFER SFP, FDP_ETC.1/SVD TRANSFER, FDP_UIT.1/SVD TRANSFER, FDP_UIT.1/TOE DTBS, FMT_SMF.1, FTP_ITC.1/SVD TRANSFER, FTP_ITC.1/DTBS IMPORT, FTP_TRP.1/TOE

6.1.5. SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing:

- Correct generation of RSA SCD/SVD pair with length of 1024 to 2048 bits (FCS_CKM.1, FMT_MSA.2), according to requirements of [5].
- The function checks correspondence between SCD/SVD prior to writing the values in an active state in the file system (FCS_COP.1/CORRESP).
- Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes.
- The random number generator of the underlying IC is used by the TOE during SCD/SVD generation.
- When new keys are generated, the old keys are overwritten on the same memory location where they were stored before (FCS_CKM.4). Key generation is protected against SPA, Timing attacks, and electromagnetic emanation (FPT_EMSEC.1).
- Hashing of data is performed using the SHA-1 and RIPEMD-160 algorithms. MAC is generated and verified using 3DES with 2 or 3 keys.

FCS_CKM.1, FCS_CKM.4, FCS_COP.1/CORRESP, FMT_MSA.2, FPT_EMSEC.1

6.1.6. SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality.

The SF.Protection function is composed of software implementations of test and security functions including:

- Self tests of the TOE (FPT_AMT.1, FPT_TST.1).
- Deletion of SCD, RAD, VAD resources when relevant memory is de-allocated (FCS_CKM.4, FDP_RIP.1).
- Validating the integrity of all key files including SCD, RAD, SVD before use and informing the Signatory when such validation fails (FDP_SDI.2/Persistent).
- Ensuring that Information is not leaked
- Performing a set of test to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1)
- Validating the integrity of the DTBS and informing the Signatory if a validation error occurs by way of an error code provided (FDP_SDI.2/DTBS)
- Initializing memory after reset
- Initializing memory of de-allocated data (FDP_RIP.1)
- Preserving secure state after sensitive processing failure (RNG, EEPROM handling) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.1, FPT_PHP.3)

FCS_CKM.4, FDP_SDI.2/Persistent, FDP_SDI.2/DTBS, FDP_RIP.1, FPT_AMT.1, FPT_FLS.1, FPT_PHP.1, FPT_PHP.3, FPT_TST.1

6.2. Assurance Measures

The assurance measures that satisfy the TOE security assurance requirements described in 5.2 are indicated in the following table. AVA_MSU.3 and AVA_VLA.4 are augmented to the EAL4 package.

Table 2 - Assurance Measures

Assurance measures Class	Component	Description
Configuration management	ACM_AUT.1	Configuration Management Documentation
	ACM_CAP.4	Configuration Management Documentation
	ACM_SCP.2	Configuration Management Documentation
Distribution and operation	ADO_DEL.2	Delivery documentation
	ADO_IGS.1	Installation, generation and start-up procedures documentation.
Development	ADV_FSP.2	External interface definition
	ADV_HLD.2	HLD document
	ADV_IMP.1	Implementation representation
	ADV_LLD.1	LLD document
	ADV_RCR.1	Correspondence analysis
	ADV_SPM.1	Security Policy model
Guidance document	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life cycle support	ALC_DVS.1	Development lifecycle documentation: - Evidential materials on security development - Definition of the life cycle of development and maintenance - Development tool and option for load dependency
	ALC_LCD.1	
	ALC_TAT.1	
Test	ATE_COV.2	Test documentation: - Test Coverage Analysis - Test Depth Analysis - Test Specification
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
Evaluation of vulnerability	AVA_MSU.3	Analysis of the erroneous use of the ASEPCOS
	AVA_SOF.1	Analysis of the security functional strength of the ASEPCOS
	AVA_VLA.4	Analysis of the vulnerability of the ASEPCOS

7. PP Claims

7.1. PP Reference

This ST claims compliance with

Title	Protection Profile — Secure Signature-Creation Device Type 3
Version	1.05
Date	Wednesday, 25 July 2001
Prepared by	ESIGN Workshop - Expert Group F
Identification	PP0006b
Approved by	WS/E-SIGN on the 30 November 2001
Registration	BSI-PP-0006-2002

7.2. PP Tailoring

Selections and refinements of SFRs allowable by SSCD PP [6] were performed and are noted by using *underline italic* text. The following SFRs from the PP have been reworked:

- Assignments:
  - FCS_CKM.1.1
  - FCS_CKM.4.1
  - FCS_COP.1.1/CORRESP
  - FCS_COP.1.1/SIGNING
  - FIA_AFL.1.1
  - FMT_MSA.1.1/ADMINISTRATOR
  - FMT_MTD.1.1
  - FMT_EMSEC.1.1
  - FMT_EMSEC.1.2
  - FPT_FLS.1.1
  - FPT_PHP.3.1
  - FTP_TRP.1.3

- Selections:
  - FPT_AMT.1.1
  - FPT_TST.1.1
  - FTP_ITC.1.2
  - FTP_TRP.1.2
  - FTP_TRP.1.3
- Refinements:
  - FDP_SDI.2.1/PERSISTENT: this PP SFR was reworded to precisely identify the

integrity mechanism provided by the TOE

- FIA_AFL.1.1: the PP SFR text was reworded to be applied to two authentication mechanisms

OT.SCD_SVD_Corresp objective for the TOE has been reworded to apply to the TOE. As per the note included in the introduction of section 4, this TOE does not provide on-demand SCD/SVD correspondence as this is provided by construction when they are generated by the TOE.

7.3. PP Additions

Following Final Interpretation 065, TOE Security Functional Requirement 5.1.4.6 Specifications of Management Functions (FMT_SMF.1) was added to the PP SFRs..

The following Security Objectives for the Environment have been added to the PP:

- OE.SOFT_DLV
- OE.DEV_TOOLS
- OE.SOFT_MECH

The following Threats have been added to the PP:

- T.SOFT_ARCHI
- T.DEV_ORG

8. Rationale

8.1. Security objectives rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

8.1.1. Security Objectives Coverage

The following able indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Table 3 - Security Environment to Security Objectives Mapping

Threats - Assumptions - Policies / Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.SOFT_DLV	OE..DEV_TOOLS	OE.SOFT_MECH
T.Hack_Phys	X			X			X	X											
T.SCD_Divulg				X															
T.SCD_Derive									X			X							
T.SVD_Forgery						X								X					
T.DTBS_Forgery										X						X			
T.SigF_Misuse										X	X				X	X			
T.Sig_Forgery	X	X		X	X	X	X	X				X	X	X		X			
T.Sig_Repud	X	X		X	X	X	X	X	X	X	X	X	X	X		X			
T.SOFT_ARCHI																		X	X
T.DEV_ORG																	X	X	
A.CGA													X	X					
A.SCA																X			
P.CSP_Qcert					X								X						
P.Qsign											X	X	X			X			
P.Sigy_SSCD			X						X		X								

8.1.2. Security Objectives Sufficiency

8.1.2.1. Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates) establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by OT.SCD_SVD_Corresp concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by OE.CGA_QCert for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures) 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 requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init provides that generation of the SCD/SVD pair is restricted to authorised users.

8.1.2.2. Threats and Security Objective Sufficiency

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. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by OT.EMSEC_Design. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing,copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by OT.SCD_Unique that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

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 TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create

SDO for data the signatory has not decided to sign, as required by the Directive [1], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. This threat is in general addressed by OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed), OE.CGA_QCert (Generation of qualified certificates), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance) and OT.Lifecycle_Security (Lifecycle security), as follows:

OT.Sig_Secure ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. OE.SCA_Data_Intend provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of OE.CGA_QCert, OT.SCD_SVD_Corresp, OT.SVD_Auth_TOE, and OE.SVD_Auth_CGA provides the integrity and authenticity of the SVD that is used by the signature verification process. OT.Sig_Secure, OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert **(**Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signaturecreation data), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory’s SCD can practically occur just once. T.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for

signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

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.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

T.SOFT_ARCHI (Corruption of software and IC designer information) deals with the corruption of program and data during development of the TOE. This is addressed by OE.DEV_TOOLS (secure software design) which ensures that the TOE is designed in a secure manner by using tools that will grant the integrity of these data. OE.SOT_MECH (software mechanisms activation) provides an additional assurance that the security of data is preserved from within the Smartcard through the activation of dedicated security features and mechanisms.

T.DEV_ORG (Corruption of software) deals with the violation of any (if existing) physical, personnel, organizational, and technical measures to corrupt the Smart Card Embedded Software during application design phase. This is addressed by OE.DEV_TOOLS (secure software design) which ensures that the TOE is designed in a secure manner, and by OE.SOFT_DLV (Secure Software Delivery) which ensures the smartcard embedded software is delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software.

8.1.2.3. Assumptions and Security Objective Sufficiency

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

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

8.2. Security Requirements Rationale

8.2.1. Security Requirement Coverage

The following able indicates the association of the security requirements and the security objectives of the TOE and its environment. The security requirements of the TOE correspond to at least one security objective of the TOE and the security requirements of the IT environment correspond to the security objectives of the environment. Moreover, some requirements correspond to the security objectives of the TOE in combination with other objectives.

Table 4 - Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.1					X				X			
FCS_CKM.4		X		X								
FCS_COP.1/CORRESP					X							
FCS_COP.1/SIGNING												X
FDP_ACC.1/SVD TRANSFER SFP						X						
FDP_ACC.1/INITIALISATION SFP			X	X								
FDP_ACC.1/PERSONALISATION SFP											X	
FDP_ACC.1/SIGNATURE CREATION SFP										X	X	
FDP_ACF.1/INITIALISATION SFP			X	X								
FDP_ACF.1/SVD TRANSFER SFP						X						
FDP_ACF.1/PERSONALISATION SFP											X	
FDP_ACF.1/SIGNATURE CREATION SFP										X	X	
FDP_ETC.1/SVD TRANSFER						X						
FDP_ITC.1/DTBS										X		
FDP_RIP.1				X							X	
FDP_SDI.2/PERSISTANT				X	X						X	X
FDP_SDI.2/DTBS										X		
FDP_UIT.1/SVD TRANSFER						X						
FDP_UIT.1/TOE DTBS										X		
FIA_AFL.1			X								X	
FIA_ATD.1			X								X	
FIA_UAU.1			X								X	
FIA_UID.1			X								X	
FMT_MOF.1				X							X	
FMT_MSA.1/ADMINISTRATOR			X	X								
FMT_MSA.1/SIGNATORY											X	
FMT_MSA.2											X	
FMT_MSA.3			X	X							X	

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FMT_MTD.1											X	
FMT_SMF.1			X	X							X	
FMT_SMR.1				X							X	
FPT_AMT.1		X		X								X
FPT_EMSEC.1	X											
FPT_FLS.1				X								
FPT_PHP.1							X					
FPT_PHP.3								X				
FPT_TST.1		X										X
FTP_ITC.1/SVD TRANSFER						X						
FTP_ITC.1/DTBS IMPORT										X		
FTP_TRP.1/TOE											X	

Table 5 - IT Environment SFRs to Environment Security Objective Mapping

Environment Security Requirement / Environment Security objectives	**OE.CGA_Qcert**	**OE.HI_VAD**	**OE.SCA_Data_Intend**	**OE.SVD_Auth_CGA**
FCS_CKM.2/CGA	x			
FCS_CKM.3/CGA	x			
FCS_COP.1/SCA HASH			x	
FDP_UIT.1/SVD IMPORT				x
FTP_ITC.1/SVD IMPORT				x
FDP_UIT.1/SCA DTBS			x	
FTP_ITC.1/SCA DTBS			x	
FTP_TRP.1/SCA		x		
R.Sigy_Name	x			

Table 6 - Assurances Requirement to Security Objective Mapping

Objectives	**Requirements**
Security Assurance Requirements	
OT.Lifecycle_Security	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, ADO_IGS.1
OT.SCD_Secrecy	AVA_SOF.1, AVA_VLA.4
OT.Sigy_SigF	AVA_MSU.3, AVA_SOF.1
OT.Sig_Secure	AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2

8.2.2. Security Requirements Sufficiency

8.2.2.1. TOE Security Requirements Sufficiency

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

OT.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. 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 attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3 and FMT_SMF.1 for static attribute initialisation. Access control is provided by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1 and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD.

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

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. 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_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_AMT.1 and FPT_FLS.1 test the working conditions of the TOE and guarantee a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, AVA_SOF HIGH by requesting strength of function high for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

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. Cryptographic correspondence is provided by FCS_COP.1/CORRESP.

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.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS IMPORT, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/SIGNATURE CREATION SFP and FDP_ACF.1/SIGNATURE CREATION SFP keep unauthorised parties off from altering the DTBS-representation.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by FIA_UAU.1 and FIA_UID.1 that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE CREATION SFP, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.

The security functions specified by FDP_SDI.2 and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functions specified by FDP_RIP.1 and FIA_AFL.1 provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AVA_MSU.3 by requesting analysis of misuse of the TOE implementation, AVA_SOF.1 by requesting high strength level for security functions, and AVA_VLA.4 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_AMT.1 and FPT_TST.1 ensure that the security functions are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD TRANSFER and FDP_UIT.1/SVD TRANSFER. The cryptographic algorithms specified by FDP_ACC.1/SVD TRANSFER SFP, FDP_ACF.1/SVD TRANSFER SFP and FDP_ETC.1/SVD TRANSFER ensure that only authorised user can export the SVD to the CGA.

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.

8.2.2.2. TOE Environment Security Requirements Sufficiency

OE.CGA_QCert (Generation of qualified certificates) addresses the requirement of qualified certificates. The functions specified by FCS_CKM.2/CGA provide the cryptographic key distribution method. The functions specified by FCS_CKM.3/CGA ensure that the CGA imports the SVD using a secure channel and a secure key access method.

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD which is provided by the trusted path FTP_TRP.1/SCA.

OE.SCA_Data_Intend (Data intended to be signed) is provided by the functions specified by FTP_ITC.1/SCA DTBS and FDP_UIT.1/SCA DTBS that ensure that the DTBS can be checked by the TOE, and FCS_COP.1/SCA HASH that provides that the hashing function corresponds to the approved algorithms.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD IMPORT. which guarantees it's integrity

8.3. Dependencies Rationale

8.3.1. Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 6.4.2 of SSCD-PP [6] for justification).

Table 7 - Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/ CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ INITIALISATION SFP	FDP_ACF.1/ INITIALISATION SFP
FDP_ACC.1/ PERSONALISATION SFP	FDP_ACF.1/ PERSONALISATION SFP
FDP_ACC.1/ SIGNATURE CREATION SFP	FDP_ACF.1/ SIGNATURE CREATION SFP
FDP_ACC.1/ SVD TRANSFER SFP	FDP_ACF.1/SVD TRANSFER SFP
FDP_ACF.1/ INITIALISATION SFP	FDP_ACC.1/ INITIALISATION SFP, FMT_MSA.3
FDP_ACF.1/ PERSONALISATION SFP	FDP_ACC.1/ PERSONALISATION SFP, FMT_MSA.3
FDP_ACF.1/ SIGNATURE CREATION SFP	FDP_ACC.1/ SIGNATURE CREATION SFP, FMT_MSA.3
FDP_ACF.1/ SVD TRANSFER SFP	FDP_ACC.1/SVD TRANSFER SFP, FMT_MSA.3
FDP_ETC.1/ SVD TRANSFER SFP	FDP_ACC.1/ SVD TRANSFER SFP
FDP_ITC.1/ DTBS	FDP_ACC.1/ SIGNATURE CREATION SFP, FMT_MSA.3
FDP_UIT.1/ SVD TRANSFER	FTP_ITC.1/SVD TRANSFER, FDP_ACC.1/SVD TRANSFER SFP
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/ SIGNATURE CREATION SFP, FTP_ITC.1/DTBS IMPORT
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/ADMINISTRATOR	FDP_ACC.1/ INITIALISATION SFP, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/SIGNATORY	FDP_ACC.1/ SIGNATURE CREATION SFP, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/ PERSONALISATION SFP, FMT_SMR.1, FMT_MSA.1/ ADMINISTRATOR, FMT_MSA.1/ SIGNATORY
FMT_MSA.3	FMT_MSA.1/ ADMINISTRATOR, FMT_MSA.1/ SIGNATORY, FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No dependencies
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	No dependencies
FPT_TST.1	FPT_AMT.1

Requirement	Dependencies
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
Functional Requirements for Certification generation application (CGA)	
FCS_CKM.2/ CGA	unsupported dependencies, see 8.3.2 for justification
FCS_CKM.3/ CGA	unsupported dependencies, see 8.3.2 for justification
FDP_UIT.1/ SVD IMPORT	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see 8.3.2 for justification ,
FTP_ITC.1/ SVD IMPORT	None
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see 8.3.2 for justification
FDP_UIT.1/ SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see 8.3.2 for justification
FTP_ITC.1/ SCA DTBS	None
FTP_TRP.1/ SCA	None

8.3.2. Justification of Unsupported Dependencies

The security functional dependencies for the TOE environment CGA and SCA are not completely supported by security functional requirements in section 5.3.

FCS_CKM.2/ CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FDP_UIT.1/ SVD IMPORT (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this PP.

FCS_COP.1/ SCA HASH	The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/ SCA DTBS	Access control (FDP_ACC.1.1) for the SCA are outside of the scope of this PP.

8.4. Security Requirements Grounding in Objectives

This chapter covers the grounding that have not been done in the precedent chapter

Table 8 - Assurance Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL 4, OT.Lifecycle_Security
ALC_LCD.1	EAL 4, OT.Lifecycle_Security
ALC_TAT.1	EAL 4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	EAL 4, OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	EAL 4, OT.SCD_Secrecy, OT.Sig_Secure,
Security Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_QCert

8.5. TOE Summary Specifications Rationale

8.5.1. Security Function Coverage

The following table covers the mapping between TSFR and TSF.

Table 9 - TOE Security Requirements to Security Function Mapping

TOE Security Functional Requirement / TOE Security Functions	SF.Acess Control	SF. Indtification and Authentication	SF.Signature Creation	SF.Secure Messaging	SF.Crypto	SF.Protection
FCS_CKM.1					x	
FCS_CKM.4					x	x
FCS_COP.1/CORRESP			x		x	
FCS_COP.1/SIGNING			x			
FDP_ACC.1/SVD TRANSFER SFP	x	x		x		
FDP_ACC.1/INITIALISATION SFP	x					
FDP_ACC.1/PERSONALISATION SFP		x				
FDP_ACC.1/SIGNATURE-CREATION SFP	x					
FDP_ACF.1/INITIALISATION SFP	x					
FDP_ACF.1/SVD TRANSFER SFP	x					
FDP_ACF.1/PERSONALISATION SFP		x				
FDP_ACF.1/SIGNATURE-CREATION SFP	x					
FDP_ETC.1/SVD TRANSFER				x		
FDP_ITC.1/DTBS	x					
FDP_RIP.1						x
FDP_SDI.2/Persistent						x
FDP_SDI.2/DTBS						x
FDP_UIT.1/SVD TRANSFER				x		
FDP_UIT.1/TOE DTBS				x		
FIA_AFL.1		x				
FIA_ATD.1		x				
FIA_UAU.1		x				
FIA_UID.1		x				
FMT_MOF.1	x					
FMT_MSA.1/ADMINISTRATOR	x					
FMT_MSA.1/SIGNATORY	x					
FMT_MSA.2			x		x	
FMT_MSA.3	x					
FMT_MTD.1	x	x				
FMT_SMF.1	x	x		x		
FMT_SMR.1	x	x				
FPT_AMT.1						x
FPT_EMSEC.1		x	x		x	
FPT_FLS.1						x
FPT_PHP.1						x
FPT_PHP.3						x
FPT_TST.1						x
FTP_ITC.1/SVD TRANSFER				x		
FTP_ITC.1/DTBS IMPORT				x		
FTP_TRP.1/TOE				x		

8.5.2 Rational for assurance measures

Each assurance requirement is covered by an assurance measure.

Table 10 - Mapping Assurance Requirements to Assurance Measures

Assurance Requirements / Assurance Measures	AM_ACM	AM_ADO	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ACM	X						
ADO		X					
ADV			X				
AGD				X			
ALC					X		
ATE						X	
AVA							X

8.6. Rationale for Extensions

The family FPT_EMSEC (TOE Emanation) is an additional family which was defined in SSCD type 3 PP [6] and was adopted here by the developer of the TOE. The family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on externally 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, etc. This family describes the functional requirements for the limitation of intelligible emanations. See also section 6.6 of [6].

8.7. Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms.

8.8. Rationale for Assurance Level 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_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

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

In **AVA_MSU.3**, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator. AVA_MSU.3 has the following dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

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

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

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. AVA_VLA.4 has the following dependencies:

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

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

8.9. PP Claims Rationale

This ST includes all the security objectives and requirements claimed by PP [6], and, all of the operations applied to the SFRs are in accordance with the requirements of the PP [6].

9. Terminology

Term	Definition
CC	Common Criteria
CIE	Carta d'Identita Elettronica
CGA	Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of the SSCD proof of correspondence between SCD and SVD and checking the sender and integrity of the received SVD.
CSP	Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in the Directive, article 2.11).
Directive	The Directive; DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
DTBS	Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes)
DTBS Representation	Data to be signed representation (DTBS-representation) means the representation data sent by the SCA to the TOE for signing and is - a hash-value of the DTBS or - an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or - the DTBS The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.
OS	Operating System
Qualified Certificate	Means a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive. (defined in the Directive, article 2.10)
RAD	Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Term	Definition
SCA	Signature-creation application (SCA) means the application used to create an electronic signature, excluding the SSCD. I.e., the SCA is a collection of application elements. - to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, - to send a DTBS-representation to the TOE, if the signatory indicates by specific non misinterpretable input or action the intend to sign, - to attach the qualified electronic signature generated by the TOE to the data or provides the qualified electronic signature as separate data.
SCD	Signature-creation data (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive, article 2.4)
SDO	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.
Signatory	Signatory means a person who holds a SSCD and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. (defined in the Directive, article 2.3)
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. (SSCD is defined in the Directive, article 2.5 and 2.6)
SVD	Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive, article 2.7)
VAD	Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user’s biometric characteristics.

10. References

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

[2] Common Criteria for Information Technology Security Evaluation — CCMB-2005-08-001 — Part 1: Introduction and general model, August 2005.

[3] Common Criteria for Information Technology Security Evaluation — CCMB-2005-08-002 — Part 2: Security functional requirements, August 2005.

[4] Common Criteria for Information Technology Security Evaluation — CCMB-2005-08-003 — Part 3: Security assurance requirements, August 2005.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

[6] PP0006b – Protection Profile — Secure Signature-Creation Device Type 3 – EAL 4+ – Version: 1.05, 25 July 2001, CWA 14169:2002 E

[7] FIPS 180-1: Secure Hash Standard - U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology - 1995 April 17

[8] Atmel AT90SC144144CT Datasheet

[9] Protection Profile PP9806 Smartcard – Integrated Circuit, version: 2.0 EAL4+

[10] Rapport de certification [XrefX], Microcontrôleur sécurisé ATMEL, AT90SC144144CT rev. [XrevX], DSSI, France, [XdateX]

[11] ETR LITE for composition - AT90SC144144CT rev. G - Toolbox version 00.03.01.04, Référence : TPG0132B

[12] JICSAP IC Card Specifications V2.0

[13] PKCS#1: RSA Cryptography Standard, Version 1.5