ASEPCOS-CNS/CIE ROM
Public Security Target

ASEPCOS-CNS/CIE with Digital Signature Application
on Atmel AT90SC12872RCFT

Version 1.0

18 July 08

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 AT90SC12872RCFT Public Security Target**
Authors:	Athena Smartcard Solutions
General Status:	Final version for certification
ST Version Number:	Version 1.0
Date of production:	18 July 2008
TOE:	ASEPCOS CNS/CIE Version 1.70 Build 001 AT90SC12872RCFT Product Identification Number: AT58803 Revision: M Atmel Toolbox Version: 00.03.01.07
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 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

ASEPCOS-CNS/CIE is embedded on Atmel AT90SC12872RCFT smart card IC evaluated to CC EAL5+ 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 and importation 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 AT90SC12872RCFT IC supporting contact and contactless interfaces. This IC is certified according to

CC EAL 5+ [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 2 Protection Profile [13] and 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 masked in ROM.

The TOE is linked to a card reader/writer via the HW and physical interfaces of the smartcard. The smartcard has contact type and contactless type interfaces.

The TOE may be applied to a contact type card reader/writer or to a contactless 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.
- The contactless type interface of the smartcard is ISO/IEC 14443 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.

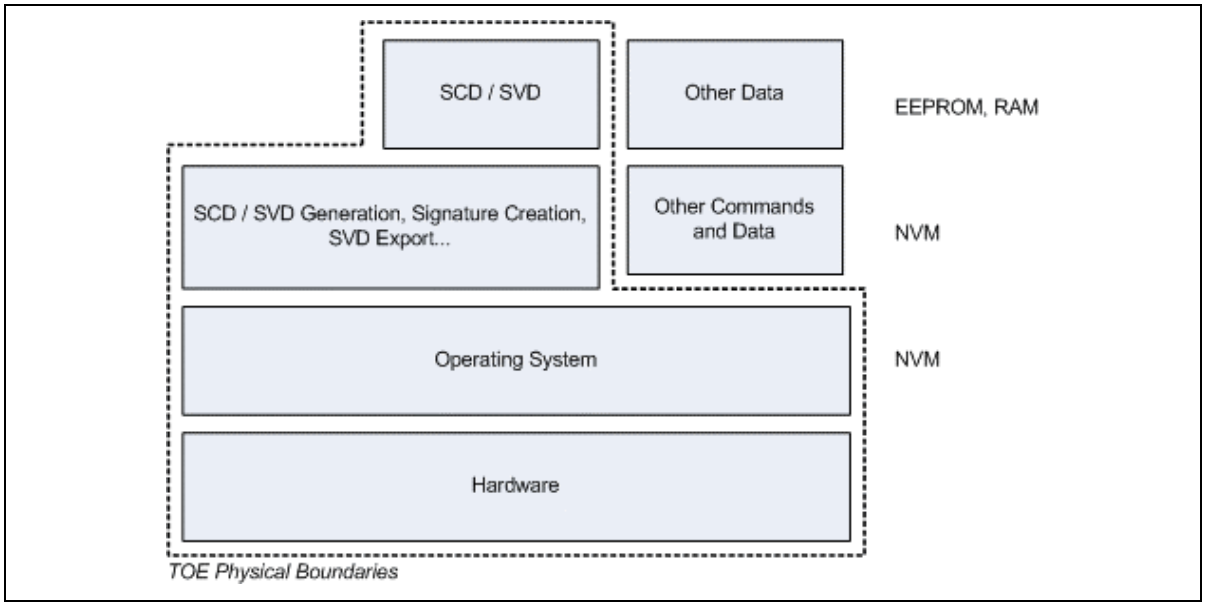


Figure 1 - TOE Description

2.2. Secure Signature Creation Devices

The following is an introduction to SSCD based on the SSCD Protection Profile [6] and [13].

The PP documents assume 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.

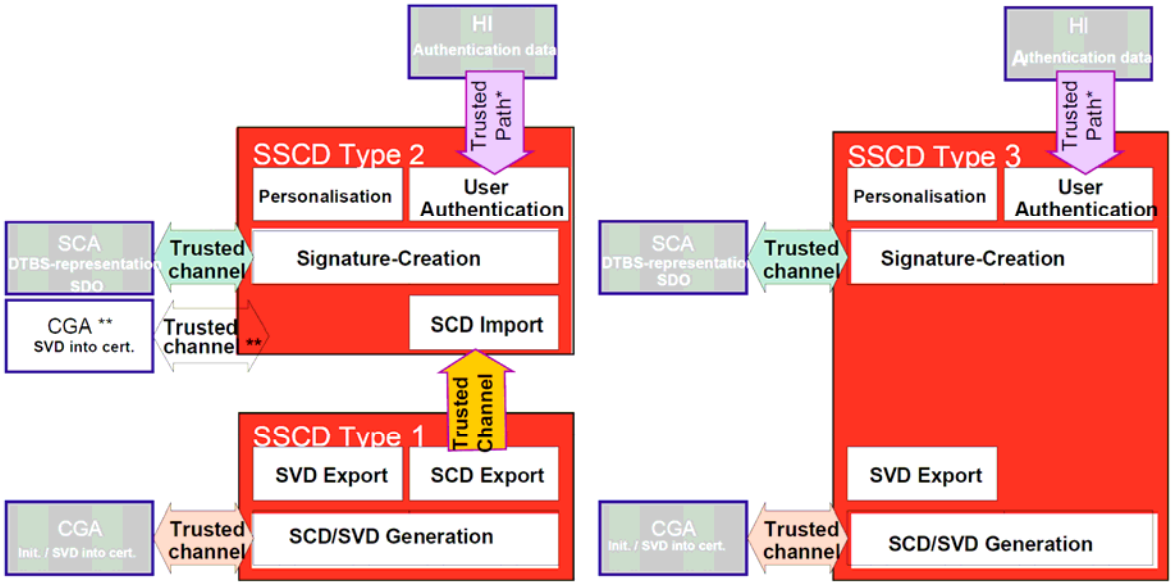
If the SSCD holds the SVD and exports the SVD to a CGA for certification, a trusted channel is to be provided. The CGA initiates SCD/SVD generation ("Init.") and the SSCD exports the SVD for generation of the corresponding certificate ("SVD into cert.").

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or 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 2 and 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)
** The trusted channel between the SSCD Type 2 and the CGA is required for cases where the SSCD type 2 holds the SVD and export of the SVD to the CGA for certification is provided

Figure 2 - SSCD types and modes of operation

2.3. Limits of the TOE

The TOE is a secure signature-creation device (combination of SSCD type 2 and type 3) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD or loads 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 ROM memory for the Atmel AT90SC12872RCFT IC.

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

(1) to store the SCD and the correspondent Signature-Verification Data (SVD)

  (a) SCD and SVD are generated by the TOE, or

  (b) SCD and SVD are imported into the TOE by an SSCD type 1

(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 generation of the SCD/SVD key pair by means of a SSCD type 1 requires the export of the SCD into the TOE (Type 2). Vice versa, signature generation by means of the TOE (Type 2) requires that the SCD/SVD has been generated by and imported from an SSCD Type 1, or has been generated by the TOE itself. Consequently, there is an interdependence where an SSCD Type 1 constitutes the environment of the TOE.

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) importation or generation of SCD/SVD pair

(2) personalization 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 3 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.

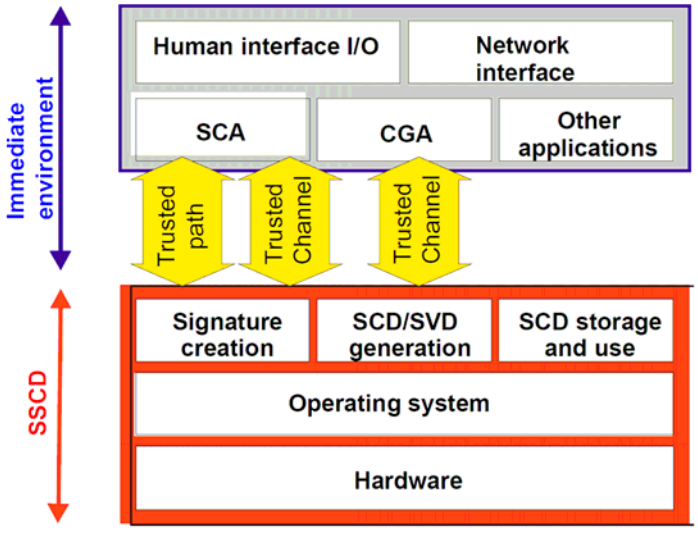


Figure 3 - Scope of the SSCD, structural view

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 4. The Life Cycle consists of a development phase and the operational phase.

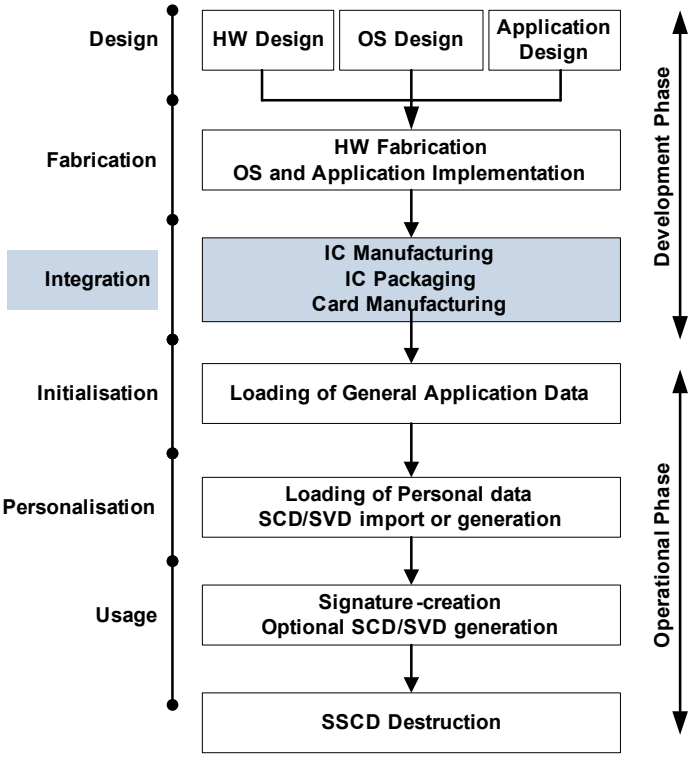


Figure 4 - SSCD life cycle

The integration phase is added to the PP generic lifecycle as this particular TOE requires that cards production phase is refined.

2.4.1. Development Phase

HW Design – Atmel

OS Design – Athena Development department – Edinburgh, Scotland

Application Design – Athena Development department – Edinburgh, Scotland

2.4.2. Fabrication phase

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.

2.4.3. Integration phase

IC Manufacturing – Atmel

IC Packaging – Atmel or specialized companies

Card Manufacturing – Atmel or specialized companies

This phase corresponds to the integration of the hardware and firmware components into the final product body. In the case of this TOE it will be a smart card, but it could also be a USB token.

The TOE is protected during transfer between various parties.

IC Packaging and Card Manufacturing are not part of the scope of this TOE.

2.4.4. Operational Phase

The chip may be sent by Atmel to Athena or to a 3rd party initialization centre/card manufacturer and Athena sends to itself or the 3rd party initialization centre the confidential information required in order to proceed with initialization. Initialization may be done in parts at various facilities (for example, start at Athena and continue in a 3rd Party or start at 3rd Party and transfer to another 3rd Party) 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 the operational phases but developed during development 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 loading of Personal Application Data and optional generation of the SCD/SVD pair if loading does not include importing an SCD/SVD pair

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.

2.4.5. 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 ROM – Informational

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

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

ASEPCOS-CNS/CIE ROM complies with ISO 7816 and ISO14443.

ASEPCOS-CNS/CIE ROM is designed to comply with the Italian CNS and CIE specification [14], the Italian Digital Signature law and the 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-CNS/CIE ROM is designed for the Atmel AVR family of smart card microprocessors and specifically the Atmel AT90SC12872RCFT IC certified according to the CC EAL 5+ [10]. ASEPCOS is protected against state of the art attacks.

The OS:

- supports ISO 14443-4 Type B, ISO 7816-4, 8 and 9 standards
- supports 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 ROM supports both CIE 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 ROM 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.

RSA signature calculation and verification according to PKCS#1 standard [12] (1024 to 2048 bits).

SHA1, SHA 256, 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 ROM supports T=1 protocol, with speeds of up to 115200 baud/s, and T=CL, with speeds up to 424000 baud/s.

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.

A.SCD_Generate *Trustworthy SCD/SVD generation*

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

(a) this party will use a SSCD for SCD/SVD-generation,
(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.
(d) The generation of the SCD/SVD is invoked by authorised users only
(e) The SSCD Type1 ensures the authenticity of the SVD it has created an exported

A.USE_Integration *Trustworthy use of SSCD during Integration phase*

It is assumed that security procedures are used during all steps of TOE integration and precisely during IC packaging and Card Manufacturing to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.DLV_integration *Trustworthy handling of SSCD during Integration phase*

It is assumed that security procedures shall ensure protection of TOE material and information under delivery and storage during all steps of TOE integration and precisely during IC packaging and Card Manufacturing to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

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 attacker 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 attack 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.

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-import or 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. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

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.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.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.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.

OT.SCD_Transfer *Secure transfer of SCD between SSCD*

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

4.2. Security Objectives for the Environment

Because ASEPCOS-CNS/CIE ROM is both SSCD type 2 and SSCD type3 means that the TOE environment consists of a CGA, an SCA, an SSCD type 1 and a specific development environment.

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alia

(f) the name of the signatory controlling the TOE,
(g) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(h) 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.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.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSVD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer *Secure transfer of SCD between SSCD*

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

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

The SSCD Type1 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.

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.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...).

OE.USE_Integration *Secure Usage of the TOE during Integration phase*

Appropriate functionality testing of the TOE shall be used during the integration phase to validate each step.
During all manufacturing and test operations, security procedures shall be used to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.DLV_Integration *Protection of TOE handling during Integration phase*

Procedures applied for delivery and storage of the TOE during the integration phase shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage
- secure storage and handling procedures (including rejected TOE's)
- traceability of TOE during delivery including the following parameters:
    - origin and shipment details
    - reception, reception acknowledgement,
    - location material/information

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 re-importation and 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.
Re-importation is not supported 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 import and on export of SVD by User.

Application note:

FDP_ACC.1/SVD Transfer SFP is only required to protect the exportation of the SVD as the SVD is never imported from an SSCD type 1 into the TOE. Actually, this TOE only provides SCD/SVD import with a fixed SVD that is known by the TOE: only SCD is transferred during an SCD/SVD import.

FDP_ACC.1.1/ SCD Import SFP	The TSF shall enforce the SCD Import SFP on Import of SCD by User.
FDP_ACC.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP on generation of SCD/SVD pair by User.
FDP_ACC.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation 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
SCD	Secure SCD import allowed	No, yes
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorized SCA	no, yes

Initialisation 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/ Initialisation 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 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.

SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP	The TSF shall enforce the SCD Import SFP to objects based on the following: General attribute and Initialisation attribute group.
FDP_ACF.1.2/ SCD Import 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” and with the security attribute “SCD / SVD management” set to “authorised” is allowed to import SCD if the security attribute “secure SCD import allowed” is set to “yes”.
FDP_ACF.1.3/ SCD Import SFP	The TSF shall explicitly authorise access of subjects to objects based On the following additional rules: none.
FDP_ACF.1.4/ SCD Import SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: (a) The user with the security attribute “role” set to “Administrator” or to “Signatory” and with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to import SCD if the security attribute “secure SCD import allowed” is set to “yes”. (b) The user with the security attribute “role” set to “Administrator” or to “Signatory” and with the security attribute “SCD / SVD management” set to “authorised” is not allowed to import SCD if the security attribute “secure SCD import allowed” is set to “no”.

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/SCD	The TSF shall enforce the SCD Import SFP when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/SCD	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: SCD shall be sent by an authorised SSCD.

Application note:

An SSCD of Type 1 is authorised to send SCD to an SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorised SSCD of Type 1 is able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

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:

An 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" (integrity redundancy code):

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

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

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

5.1.2.1. Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Receiver The TSF shall enforce the SCD Import SFP to be able to receive objects in a manner protected from unauthorised disclosure.

5.1.2.2. 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/ The TSF shall enforce the Signature-creation SFP to be able to receive the

TOE DTBS	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 the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD Import 3. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE 4. 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 channel between the TOE and a SSCD of Type 1 by means of TSF required by FTP_ITC.1/SCD import. 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 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 SCD Import SFP and Initialisation SFP to restrict the ability to modify the security attributes SCD/SVD management and Secure SCD import allowed 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 SCD Import SFP, 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 or Importation of the SCD. Also, the security Attribute of the SCD “Secure SCD import allowed” is set to “No” after creation of the SCD by the Administrator.

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 and contactless I/O* 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/ SCD 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/ SCD Import	The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD Import	The TSF or the trusted IT shall initiate communication via the trusted channel for SCD Import.
FTP_ITC.1.1/ SVD Transfer	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 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 trusted IT shall initiate communication via the trusted channel for transfer of 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 remote trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/ DTBS Import	The TSF or the trusted IT shall initiate communication via the trusted channel for signing DTBS-representation.

Refinement

The mentioned remote trusted IT products are: an SSCD type 1 for SVD import, the CGA for the SVD export, and the SCA for DTBS Import.

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 remote trusted IT product shall initiate communication via the trusted channel for import SVD.

Refinement:

The mentioned remote trusted IT product that is the TOE.

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, SHA-256 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.

data in a manner protected from modification, deletion and insertion errors.

FDP_UIT.1.2/ SCA DTBS: The TSF shall 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 remote trusted IT product shall initiate communication via the trusted channel for signing DTBS-representation by means of the SSCD.

Refinement:

The mentioned remote trusted IT product that is the TOE.

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*.

5.3.3. SSCD Type 1

5.3.3.1. 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].*

5.3.3.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1/ Type1: The TSF shall destroy cryptographic keys 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 automatically after export.

5.3.3.3. 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].

5.3.3.4. Subset access control (FCS_ACC.1)

FDP_ACC.1.1/ SCD Export SFP	The TSF shall enforce the SCD Export SFP on export of SCD by Administrator.

5.3.3.5. Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/ Sender	The TSF shall enforce the SCD Export SFP to be able to transmit objects in a manner protected from unauthorised disclosure.

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

FTP_ITC.1.1/ SCD Export	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/ SCD Export	The TSF shall permit the TSF to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD Export	The TSF or remote trusted IT product shall initiate communication via the trusted channel for SCD export.

Refinement:

The mentioned remote trusted IT product that is the TOE (being SSCD Type 2).

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 Administrator to:

- Create an initial SCD/SVD Key Pair
    - Import SCD with fixed SVD (FDP_ACC.1/SCD Import SFP, FDP_ACF.1/SCD Import SFP) from an authorised SSCD Type 1 (FDP_ITC.1/SCD Import)
    - Generate the SCD/SVD key pair
    - Export SVD (FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD Transfer SFP)
- Manage the SCD/SVD security attributes after the key pair is created (imported or generated)
    - “SCD/SVD management” is set to “not authorized” (FDP_ACC.1/Initialisation SFP, FDP_ACF.1/Initialisation SFP, FMT_MSA.1/Administrator, FMT_SMF.1)
    - “SCD Operational” is set to “No” (FMT_MSA.3)
    - “Secure SCD import allowed” is set to “No” (FMT_MSA.3)
- Create the RAD during personalisation (FDP_ACC.1/Personalisation SFP, FDP_ACF.1/Personalisation SFP)

Control over the authorization of Signatory to:

- Activate the SCD and set its operational state to “Yes” (FMT_MSA.1/Signatory, FMT_SMF.1)
- Generate a new SCD/SVD key pair
- Export SVD (FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD Transfer SFP)
- Sign DTBS data sent by an authorized SCA (FDP_ITC.1/DTBS, FDP_ACC.1/ Signature Creation SFP, FDP_ACF.1/ Signature Creation SFP, FMT_MOF.1). Any security attributes associated with the DTBS are ignored.
- Unblock and modify the RAD (FMT_MTD.1, FMT_SMF.1).

Control over the enforcement of secure messaging over:

- Export of the SVD (FTP_ITC.1/SVD Export)
- Importation of the DTBS (FTP_ITC.1/DTBS Import)
- Importation of the SCD (FTP_ITC.1/SCD Import)

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)

Administrator Authentication

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

Signatory Authentication: Activate-PIN and RAD

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.

TSF mediated actions are not allowed by the TOE before the user is identified (FIA_UID.1), authenticated and associated to the role of Signatory (FDP_ACF.1/Signature Creation SFP).

The authentication of the Signatory is made through validation of the RAD by the TOE (FIA_ATD.1, FIA_UAU.1). RAD validation consists of presentation of the VAD and comparison with the stored RAD. This is only possible if the RAD allows remaining attempts (FIA_AFL.1): each failed attempt to authenticate is counted and when maximum amount of consecutive attempts failure is reached RAD is blocked. A successful authentication resets the counter and an unblocking mechanism is provided (FMT_MTD.1.1).

Authentication data characteristics:

Authentication data	Length	Max attempts	Purpose of verification
RAD	6 bytes minimum	3	Authenticate the Signatory
PUK	6 bytes minimum	10	Unblock (set Retry Counter to initial value) or update the RAD
Activate-PIN	6 bytes minimum	3	Make Signature Creation Function operational

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.

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/SIGNING) and SHA-1, SHA-256 or RIPEMD-160 hashing calculated by SF.Crypto. The signature is calculated based on PKCS#1 version 1.5 [12].

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).

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 4 distinct channels (TOE and SSCD Type 1, TOE and 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.

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).

The SSCD Type 1, CGA, SCA and local user are allowed to initiate the communication with the TOE through via a trusted channel (FTP_TRP.1/TOE)

TOE and SSCD Type 1

During SCD Import (FTP_ITC/SCD Import), a trusted channel between the TOE and the SSCD Type 1 is established with secure messaging. Secure Messaging shall be setup to prevent disclosure of the imported SCD (FDP_UCT.1/Receiver).

TOE and CGA

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

TOE and SCA

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.

TOE and User

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

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].
- 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).
- The function checks correspondence between SCD/SVD prior to writing the values in an active state in the file system (FCS_COP.1/CORRESP).
- The random number generator of the underlying IC is used by the TOE during SCD/SVD generation.
- Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes.
- Hashing of data is performed using the SHA-1, SHA-256 or RIPEMD-160 algorithms. MAC is generated and verified using 3DES with 2 or 3 keys.

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)

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

Title	Protection Profile — Secure Signature-Creation Device Type 2
Version	1.04
Date	Wednesday, 25 July 2001
Prepared by	ESIGN Workshop - Expert Group F
Identification	PP0005b
Approved by	WS/E-SIGN on the 30 November 2001
Registration	BSI-PP-0005-2002

7.2. PP Tailoring

Selections and refinements of SFRs allowable by SSCD PP [6] and PP [13] were performed and are noted by using ***underline italic*** text. The following SFRs from the PPs 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
- FPT_TST.1.1
- FTP_TRP.1.3

Selections:

- FPT_AMT.1.1
- FPT_TST.1.1
- FTP_ITC.1.2 (all)
- FTP_TRP.1.2
- FTP_TRP.1.3

Refinements:

- FIA_AFL.1.1: the PP SFR text was reworded to be applied to two authentication mechanisms
- FMT_MSA.3.1: a restriction applies to the “Secure SCD Import allowed” security attribute

The compliancy with the two PPs (SSCD Type 2 and Type 3) has the following impact on the SFRs:

- FIA_UAU.1.1: the SFR from [13] includes the SFR from [6], adding a consideration for SCD Import
- FIA_UID.1.1: the SFR from [13] includes the SFR from [6], adding a consideration for SCD Import
- FMT_MSA.1.1/Administrator: the SFRs from [6] and [13] are not overlapping and have been merged
- FMT_MSA.3.1: the SFRs from [6] and [13] are not overlapping and have been merged
- Several SFRs are in one PP and not in the other: they are simply all enforced by the TOE

OT.SCD_SVD_Corresp objective for the TOE has been reworded to apply to the TOE. Actually, this TOE does not provide on-demand SCD/SVD correspondence as this is provided by construction when they are generated or imported on 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 PPs:

- OE.SOFT_DLV
- OE.DEV_TOOLS
- OE.SOFT_MECH
- OE.USE_Integration
- OE.DLV_Integration

The following Threats have been added to the PPs:

- T.SOFT_ARCHI
- T.DEV_ORG

The following Assumptions have been added to the PPs:

- A.USE_Integration
- A.DLV_Integration

8. 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.
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.

Term	Definition
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.

9. 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

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

[8] Atmel AT90SC12872RCFT Technical Datasheet

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

[10] Certification Report DCSSI-2008/05, ATMEL Secure Microcontroller AT90SC12872RCFT / AT90SC12836RCFT rev. M, DCSSI, France, 27th of February 2008

[11] TPG0129D – ETR LITE for composition - AT90SC12872RCFT rev. M - Toolbox version 00.03.01.07

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

[13] PP0005b – Protection Profile — Secure Signature-Creation Device Type 2 – EAL 4+ – Version: 1.04, 25 July 2001

[14] CIE Functional Specification v2.0