SafeNet eToken

-

Athena IDProtect/OS755 Java Card

on Atmel AT90SC25672RCT-USB Microcontroller

embedding IDSign applet

Security Target Lite

CC Version 3.1

Version 1.2

February 16, 2011

athena
Smartcard Solutions, INC.

SafeNet
The Foundation of Information Security

Contents

List of Tables

List of Figures

1. ST introduction

1.1. ST identification

ST title:	**- SafeNet eToken -** **Athena IDProtect/OS755 Java Card** **on Atmel AT90SC25672RCT-USB Microcontroller** **embedding IDSign applet**
Author:	Athena Smartcard Solutions
General Status:	Final version for certification
ST Version Number:	1.0
Date of production:	February 16, 2011
TOE:	Applet: Athena IDSign Version 3 Build 001 Operating System: Athena IDProtect Release Date ‘0113’ Release Level ‘0109’ Platform: AT90SC25672RCT(-USB) Product Identification Number: AT58829 Revision: D Atmel Toolbox Version: 00.03.11.05
CC Version:	3.1 - Part 1: CCMB 2006-09-001 revision 1 - Part 2: CCMB 2007-09-002 revision 2 - Part 3: CCMB 2007-09-003 revision 2
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

1.2. Composite TOE

Athena IDProtect with associated Athena IDSign applet are embedded on Atmel AT90SC25672RCT(-USB) IC with Atmel Toolbox 00.03.11.05.

1.3. ST overview

The TOE consists of the following software, Operating System and hardware parts.

Athena IDSign is an SSCD types 2 and 3 embedded application. It supports the TOE in enforcing 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 SafeNet eToken Java applet is out of scope of the TOE. This Java Card applet is used to provide cryptographic and secure storage services to the wide range of host applications via the associated SafeNet middleware layer (eToken PKI Client). This applet might share the same Security Domain [14] as the TOE IDSign Applet, but not the same package [13-JCRE]. These two applets are handled jointly by the Card Manufacturer and Personalizer: SafeNet. The TOE IDProtect Operating System enforces separation of the data between the two applets and associated packages imposing logical separation of data using the Java Card Firewall [13-JCRE].

Athena IDProtect is a GlobalPlatform 2.1.1 and Java Card™ 2.2.2 compliant Operating System that provides applets with standard services as defined in the related GlobalPlatform and Java Card specifications.

The hardware platform on which the software and Operating System are implemented is the Atmel AT90SC25672RCT(-USB) IC. This IC is certified according to CC EAL 4+ [10] with the Security Target compliant with PP9806 [9].

The embedded cryptographic toolbox is the Atmel Toolbox 00.03.11.05 and has been certified according to CC 2.3 EAL 4+ [17] with a compliancy to the CC Smartcard IC Platform Protection Profile BSI-PP-002-2001.

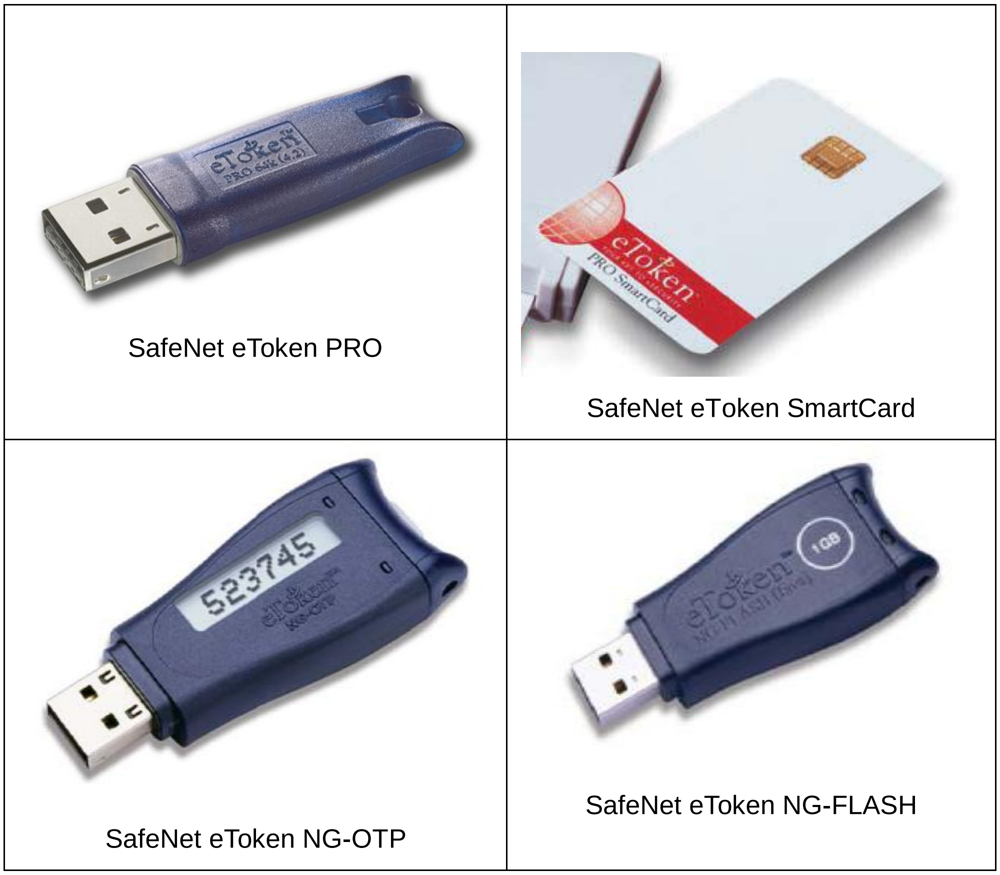
The certified form-factor is the SafeNet eToken product family including the following variants:

- eToken PRO (hardware version 4.28, firmware 2.7)
- eToken NG-OTP (hardware version 2.25, firmware 2.7)
- eToken NG-FLASH (hardware version 4.27, firmware 2.7)
- eToken SmartCard (hardware version 4.27, firmware 2.7)

2. TOE Description

2.1. General

The TOE is a Smartcard IC in the form factor of a smartcard or a USB token where digital application software is masked in ROM.



SafeNet eToken PRO

SafeNet eToken SmartCard

SafeNet eToken NG-OTP

SafeNet eToken NG-FLASH

Figure 1 – TOE Form Factor

The TOE is linked to a terminal via the HW and physical interfaces of the USB token. The TOE has only contact type USB V2.0 Full-Speed interface. ISO 7816 commands are enveloped into the vendor-specific requests (VSR) and passed from the terminal to the TOE via USB Control Transfer Endpoint 0 using the CCID, eToken or GPIO protocol.

AT90SC25672RCT(-USB) is equipped with logical peripherals including 2 timers, 1 serial port, an ISO7816 interface and an ISO7816 controller. AT90SC25672RCT(-USB) is also equipped with 1 USB interface that complies with USB v2.0, it is a full speed interface [13]

AT90SC25672RCT(-USB) can start in ISO mode or in USB mode.

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

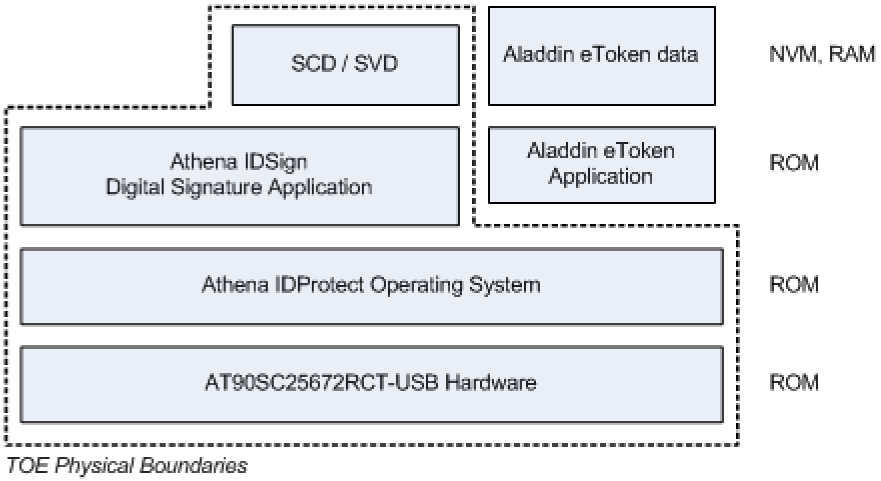


Figure 2 – TOE Description

2.2. Secure Signature Creation Devices

The following is an introduction to SSCD based on the SSCD Protection Profile [6] and [15].

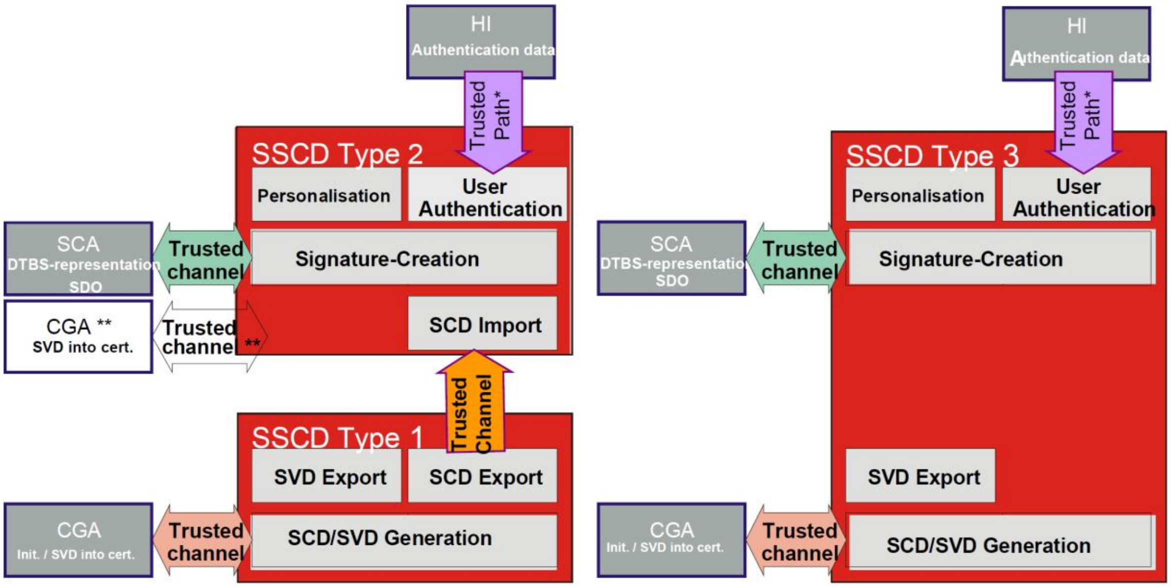
The PP documents assume a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as ‘SSCD types’, as illustrated in Figure 2.

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 3 – 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+ and embedded in a USB token which is the SafeNet eToken. The TOE includes embeddable software and two applets including the Athena IDSign applet, all in the NVM of the IC. Parts of the Operating Systems may be stored in EEPROM.

NVM (Non Volatile Memory) corresponds to ROM memory for the Atmel AT90SC25672RCT(-USB).

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 4 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.

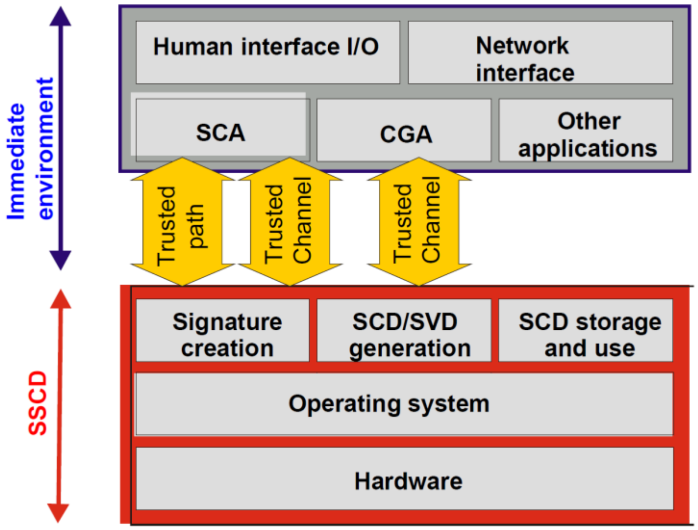


Figure 4 – Scope of the SSCD, structural view

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 Guidance

The TOE guidance comprises the following documentation:

Title	Date	Version
SafeNet eToken - Operational User Guidance	*Consult certification report for applicable dates and versions*	
SafeNet eToken - Preparative Procedures		

2.5. TOE life cycle

The TOE life cycle is shown in Figure 5. Basically, it consists of a development phase and the operational phase.

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

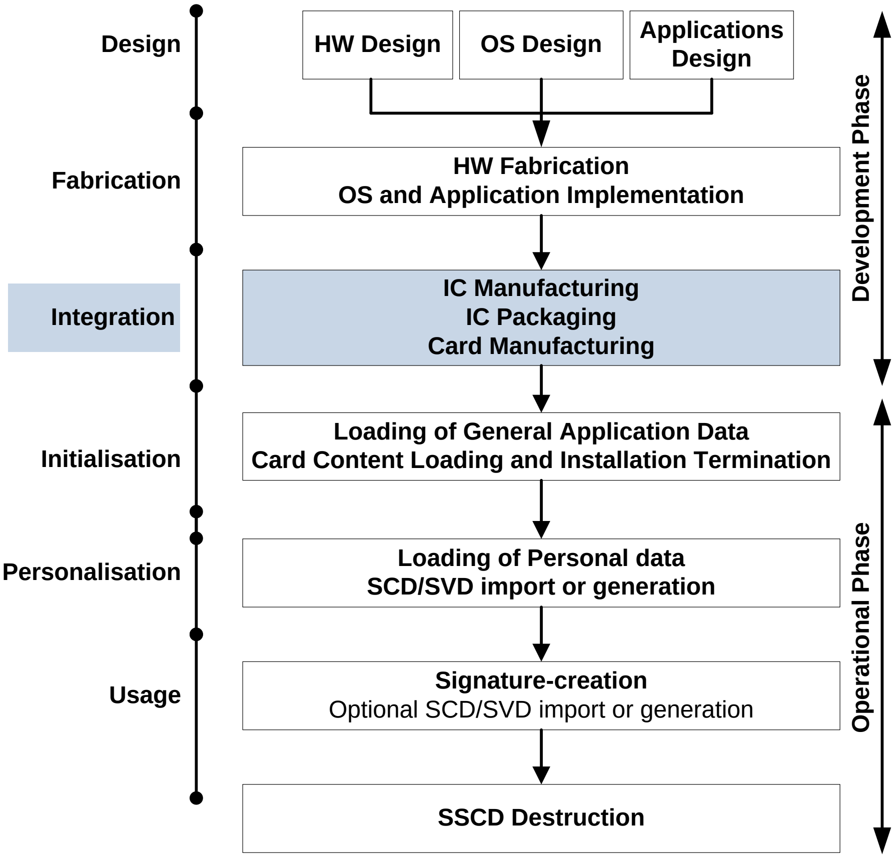


Figure 5 – SSCD life cycle

2.6. Features of IDProtect – Informational

Java promises write once, run anywhere capability. Athena IDProtect - Athena Java Card™ technology and GlobalPlatform™ Operating System - fulfils that promise for the smart card industry.

Athena's IDProtect is built to give you flexibility in the way you work: a blank canvas on which to create smart card products for all market sectors.

Central to Athena IDProtect is its compliance with the Java Card™ and GlobalPlatform™ standards; multiple compliant Java Card™ applets from any source will run securely on Athena IDProtect enabled silicon. Applets can be securely loaded and deleted post issuance thanks to GlobalPlatform™ compliant Issuer Security Domain implementation. Athena uses its RapidPort architecture to ease the process of porting the system to different silicon platforms, including contactless, meaning it is already available on various devices from leading manufacturers.

2.6.1. Java Card™

Athena IDProtect is compatible with the following Java Card standards versions:

- Runtime Environment Specification for the Java Card™ Platform, Version 2.2.2 March, 2006
- Application Programming Interface, Java Card™ Platform, Version 2.2.2 March, 2006
- Virtual Machine Specification for the Java Card™ Platform, Version 2.2.2 March, 2006

Data type int is optionally supported in the JCVM but is supported in IDProtect.

2.6.2. Global Platform

IDProtect provides a Card Manager. This is a generic term for the three card management entities of a GlobalPlatform™ card; the GlobalPlatform™ Environment, Issuer Security Domain and Cardholder Verification Method Service Provider.

Global Platform™ 2.1.1	Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
Atomic Package and Application Deletion	Memory recovered and is reusable
Global PIN	A PIN that may be checked by all applets on a card, using CVM.verify(). Its value is usually set at personalization time
Secure Channel Protocol 01	SCP01 provides mutual authentication; integrity and data origin authentication; confidentiality
Secure Channel Protocol 02	Support for all SCP02 options
Repeated application install failure	The OPEN may keep track of the number of unsuccessful consecutive attempts of the Card Content load and installation process by a particular Application and the total number of such attempts by all applications. Actions may include such defensive measures as the locking or termination of the card
Applications boundary violations	The OPEN may also enable velocity checking against repeated failed attempts by an Application to allocate additional memory beyond its allowed limit as stored in the Open Platform Registry. The OPEN may choose to lock an Application which exhibits such behaviour

2.6.3. Security settings

Keys and PINs are stored encrypted	The OS does not store any Keys or PINs in plain text during computation
On card key generation	RSA keys indicated in the Key Pair list may be generated on the card
FIPS 140-2 Level 3 (optional)	Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2, issued May 25 2001
FIPS approved secure and pseudo RNG	IDProtect supports the secure and pseudo RNG specified in JC API and are FIPS approved
FIPS 140-2 Self Tests (optional)	Power-up self tests are performed between the card power-up and the first execution of the related APDU command
FIPS 140-2 KAT (optional)	Known Answer Tests performed at power up. The cryptographic function tests consist of computing from pre-recorded input data, and comparing the results with pre-recorded answers
FIPS 140-2 Software Integrity (optional)	Checks that no FIPS application present in EEPROM (packages) is corrupted. The error detecting code is FIPS approved

2.6.4. Communication

Athena IDProtect provides the following communication features:

- Physical: ISO/IEC 7816- 1 and 2
- Electrical: ISO/IEC 7816- 3 and 4
- Protocol Support:
  - Protocol T=0 with PPS for speed enhancement
  - Protocol T=1 with PPS for speed enhancement with extended APDU length support
  - Contactless (optional) with a full support for ISO/IEC 14443 Type B protocol

2.6.5. Cryptography

Athena IDProtect is a GlobalPlatform compliant Java Card™ Operating System that supports the following cryptographic algorithms:

- RSA
  - Standard and CRT
  - RSA key pair generation
  - Used Key length: RSA_1536 to RSA_2048 bits in 32 bit increments
  - Not used Key length: RSA_512 to RSA_1504 bits in 32 bit increments
  - Algorithm: ALG_RSA_SHA_ISO9796, ALG_RSA_SHA_PKCS1, ALG_RSA_NOPAD, ALG_RSA_PCKS1
- AES: AES_128, AES_192, AES_256
- DES: Single DES, DES3_2KEY, DES3_3KEY
- Hash: SHA-1, SHA-256, and MD5
- RNG: PSEUDO and SECURE

3. Conformance Claims

3.1. CC Conformance Claim

The ST claims compliance with the following references:

- **CC Version 3.1** Part 2 [1] extended
- **CC Version 3.1** Part 3 [2]

Extensions are based on the Protection Profiles (PP [15] and PP [6]) presented in the next section:

- FPT_EMSEC.1 'TOE emanation'

The assurance level for this ST is EAL 4 augmented with: AVA_VAN.5.

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

3.2. PP Claim

This ST claims compliance with:

[15]	**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

[6]	**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

4. Security Problem Definition

4.1. 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.*

4.2. 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.

4.3. 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.**

4.4. Threats

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.MOD_SOFT *Unauthorized Software Modification*

Unauthorized modification of Smart Card Embedded Software using the patch mechanism or the Card Content Loading and Installation mechanism.

4.5. 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.

4.6. 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

5. Security Objectives

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

5.1. SOs 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.

OT.CCLI_END *Secure termination of Card Content Loading and Installation*

The TOE shall ensure that a mechanism to close the TOE in post issuance is available to the Administrator. Terminating Card Content Loading and Installation feature implies that it is not possible for an attacker to load any applet in the card using the Global Platform Card Content Management interfaces.

OT.PATCH_SEC *Secure Patch Mechanism*

The TOE must ensure continued correct operation of the patch mechanism. The TOE shall prevent the alteration of its patch mechanism: mis-routing and load of illegal patches.

OT.PATCH_END *Secure termination of Patching*

The TOE shall ensure that a mechanism to close the TOE patching mechanism is available to the Administrator. Terminating patching feature implies that it is not possible for an attacker to load any patch in the card.

5.2. SOs for the Operational 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.

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.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.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.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.

6. 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 6.1, except FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 v2.3: they are extracted from the claimed PPs which have been certified before CC v3.0 was issued. The content of the SFRs present in this ST have not been impacted by the CC v3.1: FDP_ITC.1 and FDP_SDI.1 have only been rephrased.

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 6.2 is drawn from the security assurance components from Common Criteria part 3 [4].

Section 6.3 identifies the IT security requirements that are to be met by the TOE IT environment.

The non-IT environment is described in section 6.4.

6.1. TOE Security Functional Requirements

6.1.1. Cryptographic support (FCS)

6.1.1.1. 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].*

6.1.1.2. 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.

6.1.1.3. 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].

6.1.2. User data protection (FDP)

6.1.2.1. 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.

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.

6.1.2.2. 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”.

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

FDP_ETC.1.1/
SVD Transfer

The TSF shall enforce the SVD Transfer SFP when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/
SVD Transfer

The TSF shall export the user data without the user data's associated security attributes.

6.1.2.4. 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 TOE.

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

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: SCD shall be sent by an authorised SSCD.

Application notes:

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 notes:

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.

6.1.2.5. 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.

6.1.2.6. 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 in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked persistent stored data.

FDP_SDI.2.2/
Persistent
Upon detection of a data integrity error, the TSF shall

(1) prohibit the use of the altered data
(2) inform the 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 in containers controlled by the TSF 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.

6.1.2.7. 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 user data in a manner protected from unauthorised disclosure.

6.1.2.8. 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.

6.1.3. Identification and authentication (FIA)

6.1.3.1. Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *3* unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

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

6.1.3.2. 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.

6.1.3.3. 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 notes:

"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.

6.1.3.4. 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.

6.1.4. Security management (FMT)

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

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

FMT_MOF.1.1/ Close The TSF shall restrict the ability to disable the functions Card Content Loading and Installation and Patching to Administrator.

Application notes:

The Card Content Loading and Installation particularly refers to the loading and installation of Java Card applets into the TOE. Disabling these functions is permanent: the functions are terminated.

6.1.4.2. 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.

6.1.4.3. Secure security attributes (FMT_MSA.2)

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

6.1.4.4. 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 import 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.

6.1.4.5. 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.

6.1.4.6. Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *RAD creation, RAD modification, Access Condition Management, Card Content Loading and Installation termination, Patching termination***.**

6.1.4.7. 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.

6.1.5. Protection of the TSF (FPT)

6.1.5.1. 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 I/O* to gain access to RAD and SCD.

Application notes:

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.

6.1.5.2. 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***.**

6.1.5.3. 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.

6.1.5.4. 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 SFRs are always enforced.

6.1.5.5. Testing of external entities (FPT_TEE.1)

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up* to check the fulfilment of *the correct operation of the underlying cryptography and RNG, memory initialization, and the integrity of TOE sensitive properties*.

FPT_TEE.1.2 If the test fails, the TSF shall *enter a mute state and possibly get TERMINATED*.

6.1.5.6. 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.

6.1.6. Trusted path/channels (FTP)

6.1.6.1. 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.

6.1.6.2. 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:

Once the Secure Messaging is personalized on the TOE, both Administrator and Signatory are able to establish a trusted path.

6.2. TOE Security Assurance Requirements

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

AVA_VAN is augmented from 3 to 5 compared to the CC V3.1 package for EAL4.

This augmentation in CC v3.1 complies with the augmentation required by the claimed Protection Profiles [6] and [15].

6.2.1. SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

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

Table 1 – Assurance Requirements: EAL4 augmented with AVA_VAN.5

6.2.2. SARs Rationale

The Protection Profiles that are applicable to the TOE present the mapping between the TOE Security Objectives and the SARs of CC version 2.3. The following table presents how the security assurance requirements, CC version 3.1, satisfy the TOE Security Objectives:

Objectives	Security Assurance Requirements
OT.Lifecycle_Security	*CC v2.3 = ALC_DVS.1, ALC_LCD.1, ALC_TAT.1,ADO_DEL.2, ADO_IGS.1* CC v3.1 = ALC_DVS.1, ALC_LCD.1, ALC, TAT.1, ALC_DEL.1, ALC_CMC.4, AGD_PRE.1
OT.SCD_Secrecy	*CC v2.3 = AVA_SOF.1, AVA_VLA.4* CC v3.1 = AVA_VAN.5
OT.Sigy_SigF	*CC v2.3 = AVA_MSU.3, AVA_SOF.1* CC v3.1 = AVA_VAN.5
OT.Sig_Secure	*CC v2.3 = AVA_VLA.4* CC v3.1 = AVA_VAN.5
Security Objectives	*CC v2.3 = 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* CC v3.1 = ALC_CMC.4,

Table 2 – Assurances Requirement to Security Objective Mapping

6.2.3. 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_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

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, 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_VAN.5**, an advanced analysis of the TOE is performed and establishes that the TOE is highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VAN.5 has the following dependencies:

ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.3	Basic modular design
ADV_IMP.1	Implementation representation
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures

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

6.3. Security Requirements for the IT Environment

6.3.1. Certification generation application (CGA)

6.3.1.1. 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*.

6.3.1.2. 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*.

6.3.1.3. 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.

6.3.1.4. 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.

6.3.2. Signature creation application (SCA)

6.3.2.1. 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***]

6.3.2.2. 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 be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

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

FTP_ITC.1.1/

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels

SCA DTBS

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.

6.3.2.4. 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*.

6.3.3. SSCD Type 1

6.3.3.1. 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].*

6.3.3.2. 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.

6.3.3.3. 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*].

6.3.3.4. 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.

6.3.3.5. 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.

6.3.3.6. 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).

6.4. 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.

7. TOE summary specification

7.1. TOE Security Functions

The TOE defines the following Security Functions:

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

7.2. PP Claim Rationale

This ST includes all the security objectives and requirements claimed by PP [6], PP [15], and, all of the operations applied to the SFRs are in accordance with the requirements of these PPs.

7.2.1. PP compliancy

The TOE type is compliant with the claimed PPs: the TOE is a Secure Signature-Creation Device representing the SCD storage, SCD/SVD generation, and signature-creation component.

The TOE is compliant with the representation provided in both PPS:

- SSCD of Type 1 represents the SCD/SVD generation component,
- SSCD of Type 2 represents the SCD storage and signature-creation component.
- SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel.
- SSCD Type 3 is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.
- SSCD Type 2 and Type 3 are personalized components; it means that they can be used for signature creation by one specific user – the signatory - only.

Actually, Type 2 and Type 3 are not necessarily to be considered mutually exclusive, as both PPs state.

8. Terminology

Term	Definition
Administrator	Administrator means a user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.
Advanced electronic signature	Signature (defined in the Directive, article 2.2) which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control, and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Authentication data	Information used to verify the claimed identity of a user.
CC	**Common Criteria**
Certificate	Electronic attestation which links the SVD to a person and confirms the identity of that person (defined in the Directive, article 2.9).
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).
CWA	**CEN Workshop Agreement** (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN).
Directive	The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures.
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 - the DTBS The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value is calculated by the SCA. The final hash-value in the other case is calculated by the TOE. This TOE does not have the capability to support an intermediate hash-value.
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)

Term	Definition
Qualified Electronic Signature	Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive, article 5, paragraph 1.
RAD	**Reference Authentication Data** (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user in the role of ‘Signatory’. The operations supported by the RAD are: creation, modification, AC Management, authentication, block, unblock, and de-allocation.
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). The operations supported by the SCD are: creation, import, generation (together with the SCD), activation, data signature and de-allocation.
SCS	**Signature Creation system** (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.
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)
Signature attributes	Information that is signed together with the user message.
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)
SSCD Provision Service	Service that prepares and provides a SSCD to subscribers.
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). The operations supported by the SCD are: creation, import, export, generation (together with the SCD), activation and de-allocation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
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-2006-09-001 — Part 1: Introduction and general model, September 2006.

[3] Common Criteria for Information Technology Security Evaluation — CCMB-2007-09-002 —Part 2: Security functional requirements, September 2007.

[4] Common Criteria for Information Technology Security Evaluation — CCMB-2007-09-003 —Part 3: Security assurance requirements, September 2007.

[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 2006/30, ATMEL Secure Microcontroller AT90SC25672RCT-USB rev. D, DCSSI, France, 19 December 2006

[11] ETR LITE for composition - AT90SC25672RCT-USB rev. D - Toolbox version 00.03.01.04, Référence : TPG0140A

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

[13] Java Card 2.2.2 Specification. March 2006. Published by Sun Microsystems, Inc.

- Virtual Machine Specification [JCVM]
- Application Programming Interface [JCAPI]
- Runtime Environment Specification [JCRE]

[14] Global Platform, Card Specification, Version 2.1.1, March 2003

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

[16] CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007

[17] Security Target Lite - Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices – TPG0177 Version: A, 19 December 2008