IDProtect Duo v9 SSCD – Security Target Lite

Athena IDProtect/OS755 Java Card
On STMicroelectronics SB23YR48/80B Microcontroller
Embedding Athena IAS-ECC applet

Version: 1.4

Date: 10 December 2014

athena Smartcard

Athena Smartcard Inc., 16615 Lark Ave, Suite 202, Los gatos CA 95032

Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Identification

ST Lite title	**- Athena IDProtect Duo v9SSCD - Athena IDProtect/OS755 Java Card on STMicroelectronics SB23YR48/80B Microcontroller embedding IAS-ECC applet**
Authors	Athena Smartcard, Inc.
General Status	Final
ST Version Number	1.4
Date of production	December 10, 2014
TOE Reference	Mask Reference: "SmartGrid_ST23YR80_001_P1_FA" IASECC Applet Athena Smartcard Solutions, Inc. Version 0003 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code reference: "vFA03 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 4016 Release Level 0101 ROM Code reference: "SmartGrid_ST23YR80_001" EEPROM Code reference: "SmartGrid_ST23YR80_001_P1" SB23YR48/80B STMicroelectronics Revision H or I Configuration SB Maskset K2M0A Certificate ANSSI-CC-2012/68 [9] NesLib STMicroelectronics Version 3.0 Certificate ANSSI-CC-2012/68 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
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

[9] ANSSI-CC-2012/68 " *Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB - Référence : maskset K2M0A, révision externe B, révision interne H ou I*".

CC v3.1 Rev 3, EAL 6+ (ALC_FLR.1), compliant to BSI-PP-0035-2007 version 1.0.

1.2. Composite TOE

In this Security Target, the name of the composite TOE developer (Athena Smartcard Solutions, Inc.) will be referenced as 'Athena'.

IDProtect with associated IAS-ECC applet are embedded on STMicroelectronics SB23YR48/80B IC.

The composition analysis conducted in this section will use the words Platform to designate the STMicroelectronics SB23YR48/80B IC [6, 7], Application to designate the two software components Athena IDProtect/OS755 and Athena IAS-ECC Applet, and Composite Product to designate the TOE.

According to the Composite product documentation [14], the different roles considered in the composition activities are associated as follows:

Platform Developer	STMicroelectronics
Platform Evaluator	Serma Technologies
Platform Certification Body	ANSSI
Application Developer	Athena
Composite Product Integrator	STMicroelectronics
Composite Product Evaluator	Serma Technologies
Composite Product Certification Body	ANSSI
Composite Product evaluation Sponsor	Athena

See composition requirements coverage:

[R1] Platform was evaluated to CC EAL 6+ according to BSI-PP-0035-2007 [8] and Composite Product ST relies on this claim.

[R2] Platform Security Target [10] is available.

[R3] Evaluated versions of the Platform and Application are exposed here in section 1.1.

[R4] Integration evidences are provided as part of the process.

[R5] Integration is guided by delivery procedures enforced by Athena and STMicroelectronics.

[R6] Integration process involves all configuration parameters provided by Athena.

[R7] Integration data and processing are tracked by Athena.

[R8] Application development process incorporates the Platform User Guide as technical input.

[R9] EAL 6+ certification of the Platform provides:
- List of applicable Technical Guides, Application Notes and Errata Sheets
- Certified Platform ETR
- Platform Certification Report [9]

[R10] TOE Test Plan describes validation of the Application on Platform dedicated emulator.

[R11] TOE Test Plan describes validation of the Application on the Platform.

[R12] Platform certification includes testing evaluation.

[R13] Platform samples are delivered by STMicroelectronics to TOE's evaluator for testing purpose.

[R14] Composite Product samples are delivered by STMicroelectronics to TOE's evaluator for penetration testing purpose.

[R15] Platform open samples are delivered by STMicroelectronics to TOE's evaluator for testing purpose.

[R16] EAL 6+ certification of the Platform provides Certified Platform ETR and Certification Report.

1.3. TOE Overview

The TOE implements a Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [15] 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.

IDProtect Duo v9 is a multi-application Java Card which supports RSA cryptography of up to 4096.

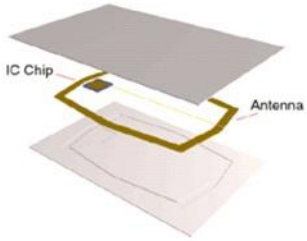
The TOE meets all the following requirements as defined in the European Directive (article 2.2):

(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

2. TOE Description

2.1. General

The TOE is available in a variety of form factors where digital application software is masked in ROM:

<table>
<tr><td colspan="3">1. Contactless interface cards and modules</td></tr>
<tr><td colspan="3"> 

(antenna embedded in plastic)</td></tr>
<tr><td colspan="2">2. Dual interface cards and modules</td><td>3. Contact only cards and modules</td></tr>
<tr><td colspan="2"> 
(antenna embedded in plastic)</td><td> 

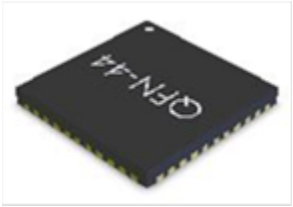
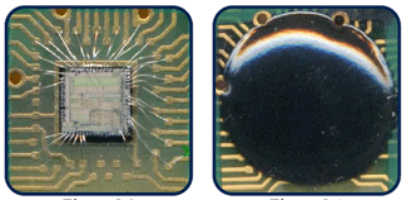
(contactless interface absent or disabled)</td></tr>
<tr><td>4. SOIC8 package</td><td>5. QFN44 package</td><td>6. Chip on Board (PCB)</td></tr>
<tr><td> 
</td><td> 
</td><td>  </td></tr>
</table>

Figure 1 – TOE Form Factor

The TOE is linked to a card reader/writer via its HW and physical interfaces.

- The contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.
- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The interfaces of the TOE QNF-44 are JEDEC compliant.

There are no other external interfaces of the TOE except the ones described above.

The antenna and the packaging are both out of the scope of this TOE.

The TOE smartcard form factors may be applied to a contact type card reader/writer or to a contactless card reader/writer when the contactless interface of the smartcard is available. The card reader/writer is connected to a computer such as a personal computer and allows application programs (APs) to use the TOE.

2.2. TOE Boundaries

The TOE boundaries are the following:

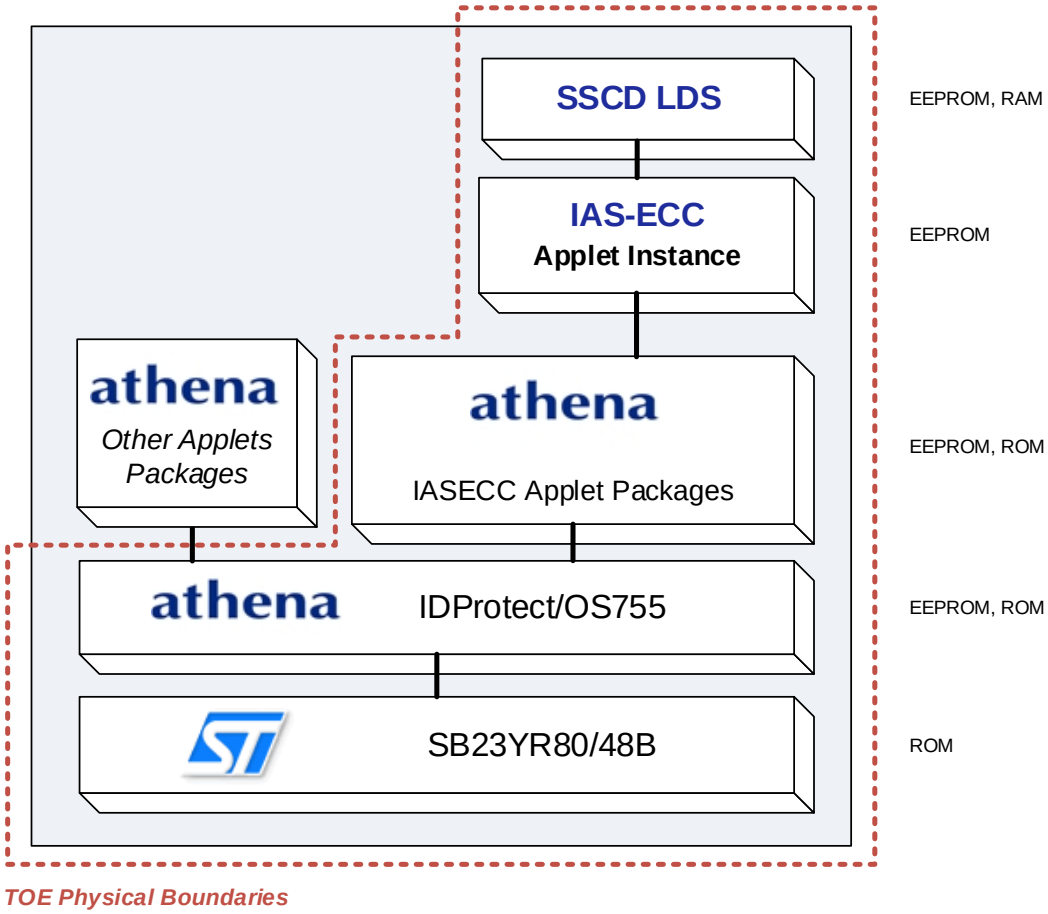


Figure 2 – TOE Boundaries

Other applet packages are present on the chip in ROM: Athena LASER applet and Athena MiniDriver applet. They can be instantiated for testing only. The IASECC Applet package could be instantiated into an ICAO applet instance or an IAS-ECC applet instance. Only the IAS-ECC applet instance is part of the TOE. Other applets are not instantiated on this TOE.

In a general aspect, IDProtect Operating System enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card™ Firewall [11-JCRE]. LASER is a Digital Signature Java Card application and follows the ISO7816 standard. LASER is not instantiated in the final product and therefore is out of the scope of this TOE.

IAS-ECC Applet can also be instantiated in ICAO mode, and is then out of the scope of this TOE in this mode.

Athena IDProtect duo v9 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 [13] and Java Card specifications [12].

The portions of the Applet Packages and Operating System present in EEPROM are the patches.

The hardware platform on which the Operating System is implemented is the STMicroelectronics SB23YR48/80B IC. This IC is certified according to CC EAL 6+ [9] with the Security Target compliant with BSI-PP-0035-2007 [8].

2.3. IAS-ECC - Secure Signature Creation Device

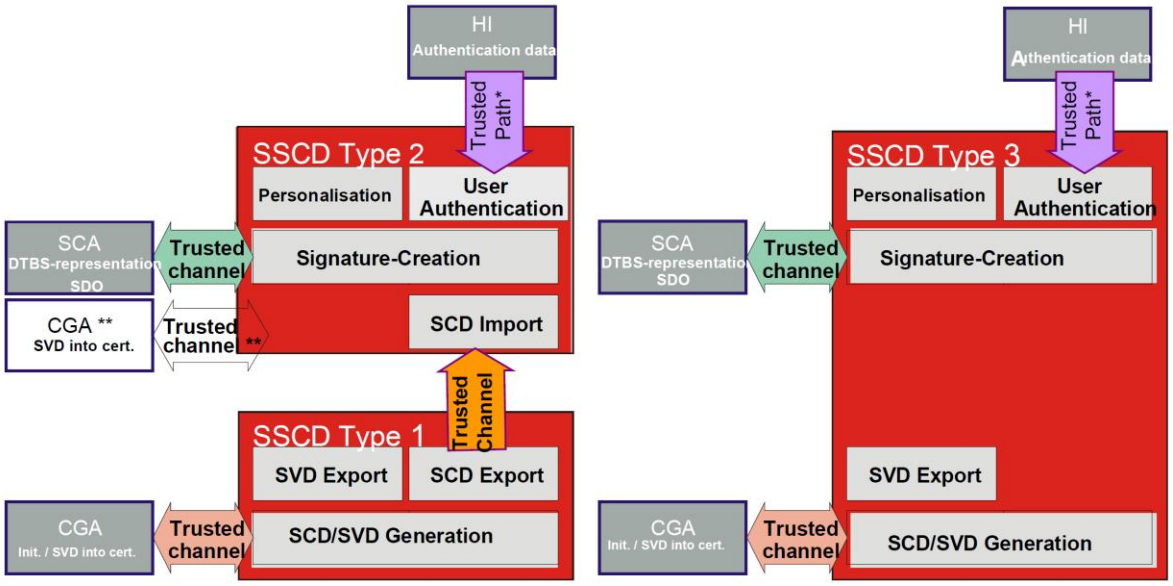
The following is an introduction to SSCD based on the SSCD Protection Profile [4] and [5].

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). If 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

2.4. TOE Limits

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 [15].The destruction of the SCD is mandatory before the TOE generate a new pair SCD/SVD or loads a new pair SCD/SVD.

A SSCD is configured software or hardware used to implement the signature-creation data (SCD). 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.

The TOE described in this ST is a smart card operating system implemented on a smart card IC which is certified CC EAL 6+. 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 STMicroelectronics SB23YR48/80B IC [10, 8].

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

(1) to generate the SCD and the correspondent signature-verification data (SVD)
(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 interdependence where an SSCD Type 1 constitutes the environment of the TOE.

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The TOE may provide an interface for user authentication by its own or implements IT measures to support a trusted path to a trusted human interface device.

This TOE does not implement, in addition to the functions of the SSCD, the signature-creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. The SCA 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 initialised for the signatory's use by

(1) importation of the SCD or generation of SCD/SVD pair
(2) personalization for the signatory by means of the signatory’s verification authentication data (VAD)

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if the SCD is no longer used for signature generation.

The TOE allows to implement a Human Interface (HI) for user authentication:

(i) by the TOE itself or

(ii) by a trusted human interface device connected via a trusted channel with the TOE.

The human interface device is used for the input of VAD for authentication by knowledge or for the

generation of VAD for authentication by biometric characteristics. The TOE holds RAD to check the provided VAD. The human interface implies appropriate hardware. The second approach allows to reduce the TOE hardware to a minimum e. g. a smart card.

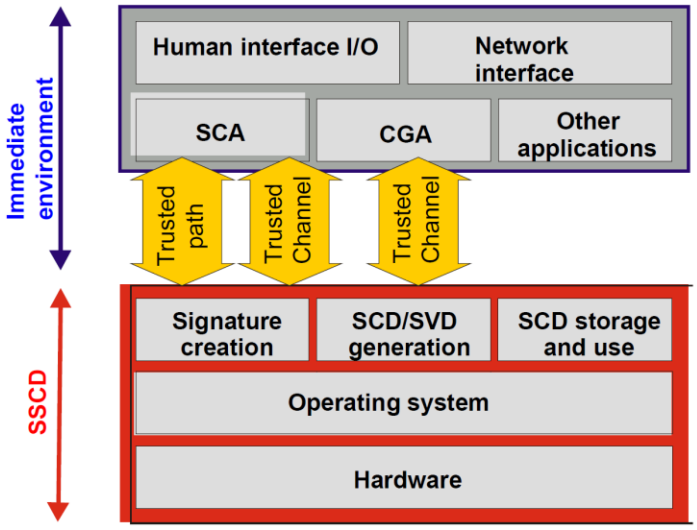


Figure 4 – Scope of the SSCD, structural view

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.

2.5. TOE Guidance

The TOE guidance comprises the following documentation:

Title	Date	Version
IDProtect Duo v9 – Manufacturer Manual	*Consult certification report for applicable dates and versions*	
IDProtect Duo v9 SSCD - Preparative Procedures		
IDProtect Duo v9 SSCD - Operational User Guidance		

2.6. TOE lifecycle

The TOE lifecycle is shown in Figure 5.

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

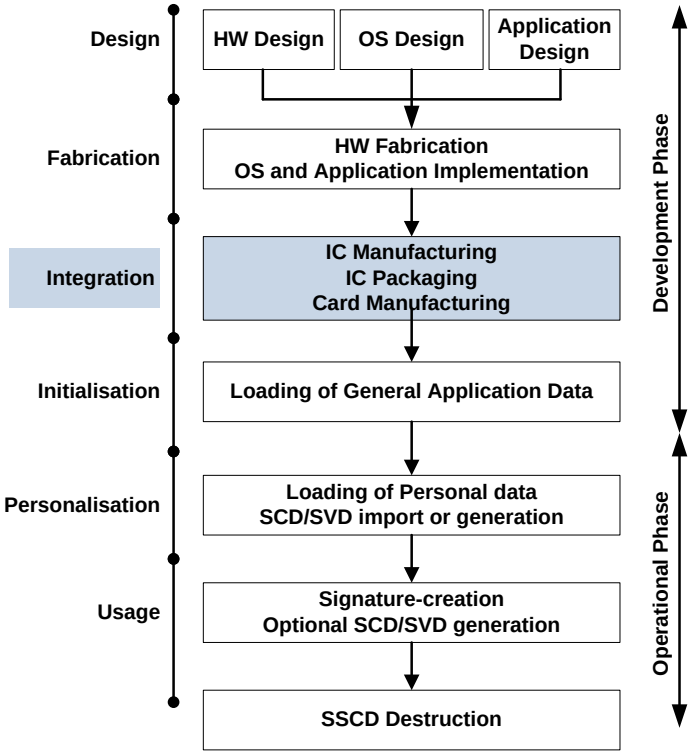


Figure 5 – TOE lifecycle

2.6.1. Design Phase

The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

HW Design – STMicroelectronics

OS Design – Athena Development departments – Los Gatos, US
– Livingston, Scotland

Application Design – Athena Development departments – Los Gatos, US

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the IDProtect Duo v9 application and the guidance documentation is securely delivered to the IDProtect Duo v9 manufacturer.

2.6.2. Fabrication Phase

HW Fabrication and OS & Application implementation – STMicroelectronics

IC Manufacturing – STMicroelectronics

The Operating System and applicative parts of the TOE which are developed by Athena are sent in a secure way to STMicroelectronics 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. Additional Java Card applets developed by Athena are included in the mask and the corresponding converted files (.cap or.jca) are also provided to STMicroelectronics.

2.6.3. Integration Phase

The Integration Phase is performed under the assurance when the TOE components have to be Initialized. In this case, all the steps of Integration are performed by STMicroelectronics.

When the Initialization Phase is not required, any TOE material that enters the Integration Phase is already pre-personalized: the patches have already been applied (if any), the Patch Mechanism has been Terminated, the applications have been instantiated as required by the TOE configuration, the Card Content Loading and Installation mechanism has been Terminated, and the TOE is ready for personalization. In this case, the TOE is outside of the assurance when it enters the Integration Phase.

IC Manufacturing – STMicroelectronics

IC Packaging – STMicroelectronics

Card Manufacturing – STMicroelectronics

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 with a diversified (per card) Transport Key.

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

2.6.4. Initialization Phase

In order to proceed with initialization, the chip may be sent by STMicroelectronics to Athena, or Athena sends to STMicroelectronics the confidential information required to complete this phase. Initialization may be done in parts at various facilities, under the governance of Athena and STMicroelectronics. The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.

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

Creation of the application implies applet instantiation and the creation of MF and IAS-ECC ADF. It is not the case of this TOE, but applets could be loaded in the TOE at this point. Card Content Loading and Installing mechanism is terminated in this phase.

2.6.5. Personalization Phase

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

The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.

The Personalization phase is not part of the scope of this TOE.

2.6.6. Operational Phase

This ST addresses the functions used in the operational phases but developed during development phase.

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.

The Operational Use phase is not part of the scope of this TOE.

2.6.7. 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 [15].

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 [15], 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.

2.7. 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.

2.7.1. GlobalPlatform

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.

GlobalPlatform 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
Secure Channel Protocol 03	Support for all SCP03 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 behavior

2.7.2. Java Card

Athena IDProtect is compatible with the following Java Card standards versions [12]:

- 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 and is supported in IDProtect.

2.7.3. 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	Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2
FIPS approved DRBG	IDProtect supports the secure RNG specified in JC API and is FIPS approved
FIPS 140-2 Self Tests	Self tests are performed to check that the HRNG and the DRBG are not stuck and that RSA Keys that are generated by the TOE are a consistent pair.
FIPS 140-2 KAT	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	Checks that no FIPS application present in EEPROM (packages) is corrupted. The error detecting code is FIPS approved

2.7.4. Cryptography

Athena IDProtect is a GlobalPlatform compliant Java Card [12] Operating System that supports the cryptographic algorithms.

Note that not all the Cryptographic algorithms, lengths and modes are involved in TOE Security Functions. Please refer to the relevant SFRs for a complete description of what cryptography is used by the TOE (section 7.1.1).

Supported Cryptographic Algorithms (non-SFR enforcing ones in italic):

- AES: AES_128*, AES_192, AES_256*
- DES: 2 keys TDES [22], *Single DES*, 3 *keys TDES*,
- *ECC:*
  - *Finite Prime Field*
  - *ECC key pair generation*
  - *Key length:* *160 to 521 bits*
  - *Algorithm:* *ALG_ECDSA_SHA, ALG_ECDSA_SHA_224, ALG_ECDSA_SHA256*
- RSA
  - CRT *and Standard*
  - RSA key pair generation
  - Used Key length: RSA_1024 to RSA_2048, *and up to RSA_4096 bits*
  - Algorithm: ALG_RSA_SHA_PKCS1, ALG_RSA_SHA256_PKCS1, *ALG_RSA_SHA_ISO9796 [18], ALG_RSA_NOPAD, ALG_RSA_SHA_PKCS1_PSS, ALG_RSA_SHA256_PKCS1_PSS, ALG_RSA_PCKS1*
- Hash: SHA-1, SHA-256, *SHA-224, SHA-384, SHA-512*
- RNG: True RNG and FIPS compliant DRNG

2.7.5. 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 with a full support for ISO/IEC 14443 Type B protocol

3. Conformance Claims

3.1. CC Conformance Claim

The ST claims compliance with the following references:

- Common Criteria Version 3.1 Part 1 [1]
- Common Criteria Version 3.1 Part 2 [2] extended
- Common Criteria Version 3.1 Part 3 [3] conformant

Extensions are based on the Protection Profiles (PP [4] and PP [5]) presented in the next section:

- FPT_EMSEC.1 'TOE emanation'

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

- AVA_VAN.5
- ALC_DVS.2

3.2. PP Claim

This ST claims strict compliance to the following Protection Profiles:

[4]	**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

[5]	**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**: RAD, 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**: Code of the SSCD dedicated to the generation of digital signature of DTBS 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**: output of the Signature-creation function (Unforgeability of electronic signatures must be assured).

4.2. Subjects

This Security Target considers the following 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. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used:

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

4.4. Threats

4.4.1. Threat agents

S.OFFCARD	Attacker. A human or 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.**

4.4.2. 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.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.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 being 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.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. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

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.

5. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

5.1. SOs for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by 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.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_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.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 GlobalPlatform Card Content Management interfaces.

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 Environment

Because IDProtect Duo v9 SSCD 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.

5.3. Security objectives rationale

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

5.3.1. Security Objectives Coverage

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

Threats Assumptions Policies / Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.SCD_Transfer	OT.CCLI_END	OT.PATCH_END	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique
T.Hack_Phys	x			x			x	x														
T.SCD_Divulg				x									x								x	
T.SCD_Derive									x			x										x
T.SVD_Forgery						x											x					
T.DTBS_Forgery										x									x			
T.SigF_Misuse										x	x							x	x			
T.Sig_Forgery	x	x		x	x	x	x	x				x	x			x	x		x	x	x	
T.Sig_Repud	x	x		x	x	x	x	x	x	x	x	x	x			x	x		x	x	x	
T.MOD_SOFT														x	x							
A.CGA																x	x					
A.SCA																			x			
A.SCD_Generate																				x	x	x
P.CSP_Qcert					x											x				x		
P.Qsign											x	x				x			x			
P.Sigy_SSCD			x						x		x											x

Table 1 – Security Environment to Security Objectives Mapping

5.3.2. Security Objectives Sufficiency

5.3.2.1. Policies and Security Objective Sufficiency

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

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [15], article 5, paragraph 1. Directive [15], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

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

5.3.2.2. Threats and Security Objective Sufficiency

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

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [15], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation. OT.SCD_Transfer and OE.SCD_Transfer ensures the confidentiality of the SCD transferred between SSCDs.

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

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. T.SVD_Forgery is addressed by OT.SVD_Auth_TOE which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by OE.SVD_Auth_CGA which provides verification of SVD authenticity by the CGA.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [15], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

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

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

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

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OT.Sig_Secure, OT.SCD_Transfer, OT.SCD_Secrecy, OT.Tamper_ID, OT.Tamper_Resistance, OT.EMSEC_Design, and OT.Lifecycle_Security ensure the confidentiality of the SCD implemented in the signatory's SSCD. OT.Sigy_SigF provides that only the signatory may use the TOE for signature generation. OT.Sig_Secure ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. OE.SCA_Data_Intend and OT.DTBS_Integrity_TOE ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

The threat **T.MOD_SOFT "Unauthorized Software Modification"** deals with the alteration of loaded and installed software or more generally Applicative Card Content. This threat is in general addressed by OT.CCLI_END, and OT.PATCH_END. OT.CCLI_END guarantees that the Card Content Loading and Installing mechanism is no longer available once it is terminated which prevents the addition of software applications or packages. OT.PATCH_END guarantees that the patch loading is no longer available once it is terminated.

5.3.2.3. Assumptions and Security Objective Sufficiency

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

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

A.SCD_Generate (Trustworthy SCD/SVD generation) establishes a trustworthy SCD/SVD pair. This that the SCD must be unique, objective met by OE.SCD_Unique, that the SCD and the SVD must correspond, objective met by OE.SCD_SVD_Corresp. The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, OE.SCD_Transfer.

6. Extended Components Definition

This ST contains the following extended component defined as extension to CC part 2 in the claimed PPs [4,5]:

- SFR FPT_EMSEC.1 'TOE emanation'

6.1. TOE emanation (FPT_EMSEC.1)

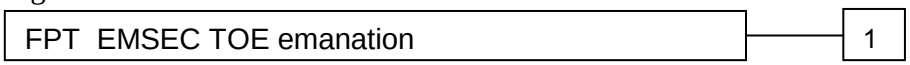
The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE Emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not to emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

7. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.
Security functional requirements components given in section 7.1, 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 [2]. Operations for assignment, selection and refinement have been made and are designated by an underline, in addition, where operations that were uncompleted in the PPs are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 0 is drawn from the security assurance components from Common Criteria part 3 [3].

7.1. TOE Security Functional Requirements

7.1.1. Cryptographic support (FCS)

7.1.1.1. 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 [16]*.

7.1.1.2. 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 note:

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.

7.1.1.3. 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 [16].*

FCS_COP.1.1/ SIGNING The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *1024 bit, 1536 bit and 2048 bit* that meet the following: *RSA CRT with hashing SHA-1 or SHA-256 and with padding PKCS#1 v1.5 as per Algorithms and parameters for algorithms [16].*

FCS_COP.1.1/ ENC The TSF shall perform *data encryption/decryption for Administrator and Signatory authentication and Secure Messaging* in accordance with a specified cryptographic algorithm *TDES CBC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [22]*.

FCS_COP.1.1/ MAC The TSF shall perform *Message Authentication Code for Secure Messaging* in accordance with a specified cryptographic algorithm *TDES MAC* and cryptographic key sizes *16 bytes* that meet the following: *FIPS PUB 46-3 Data Encryption Standard (DES) [22]*.

7.1.2. User data protection (FDP)

7.1.2.1. 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.

7.1.2.2. 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.1.4/ 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.1.4/ 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.1.4/ 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.1.4/ 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.1.4/ 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".

7.1.2.3. 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.

7.1.2.4. 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.1.4/ 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 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.1.4/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 TOE.
FDP_ITC.1.2/ DTBS	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.4/ DTBS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: 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.1.4/SCA DTBS.

7.1.2.5. 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.

7.1.2.6. 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)
4. Corrective patch code and data

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 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.

7.1.2.7. 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.

7.1.2.8. 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.

7.1.3. Identification and authentication (FIA)

7.1.3.1. Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *10 consecutive* unsuccessful authentication attempts occur related to: *RAD authentication and PUK authentication*.

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

7.1.3.2. 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.

7.1.3.3. 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.

7.1.3.4. 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.

7.1.4. Security management (FMT)

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

FMT_MOF.1/ Sign The TSF shall restrict the ability to enable the functions signature-creation function to Signatory.

FMT_MOF.1/ Patch The TSF shall restrict the ability to *disable* the functions *Patching* to *Administrator*.

FMT_MOF.1/ CCLI The TSF shall restrict the ability to *disable* the functions *Card Content Loading and Installation* to *Administrator*.

7.1.4.2. 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.

7.1.4.3. Secure security attributes (FMT_MSA.2)

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

7.1.4.4. 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.

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.

7.1.4.5. 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.

Application note:

The RAD can be unblocked by the Signatory after presentation of the PUK by the Signatory. in case of a PIN. In case of a DES Key, the RAD cannot be unlocked.

7.1.4.6. 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, Patching termination, Card Content Loading and Installation termination*.

7.1.4.7. 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.

7.1.5. Protection of the TSF (FPT)

7.1.5.1. 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 *any user* 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.

7.1.5.2. 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: *IC sensors failure detection (RNG failure, EEPROM failure, out of range temperature, clock and voltage of chip)*.

7.1.5.3. 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.

7.1.5.4. Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *Environment attacks (clock frequency and voltage tampering) and Intrusive attacks (penetration of the module protective layers)* to the *IC Hardware* by responding automatically such that the SFRs are always enforced.

7.1.5.5. 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.1.4 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

7.1.6. Trusted path/channels (FTP)

7.1.6.1. 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.1.4/ 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.1.4/ 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.1.4/ 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.

7.1.6.2. 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.1.4/ 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.

7.2. TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 5.2 of the claimed PPs [4,5].

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 PPs.

ALC_DVS is augmented from 1 to 2, compared to the CC V3.1 package for EAL4. This augmentation in CC v3.1 complies with the augmentation required by the claimed PPs.

7.2.1. 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: Lifecycle 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.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle 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 2 – Assurance Requirements: EAL4 augmented

7.2.2. SARs Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

AVA_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OT.AA_Proof.

The component 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

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 has no dependencies.

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

7.3. Security Requirements Rationale

7.3.1. Security Requirement Coverage

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

TOE SFRs / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.SCD_Transfer	OT.CCLI_END	OT.PATCH_END
FCS_CKM.1					X				X						
FCS_CKM.4		X		X									X		
FCS_COP.1/CORRESP					X										
FCS_COP.1/SIGNING												X			
FCS_COP.1/ENC													X		
FCS_COP.1/MAC										X			X		
FDP_ACC.1/SVD TRANSFER SFP						X									
FDP_ACC.1/INITIALISATION SFP			X	X											
FDP_ACC.1/PERSONALISATION SFP											X				
FDP_ACC.1/SIGNATURE CREATION SFP										X	X				
FDP_ACC.1/SCD IMPORT SFP													X		
FDP_ACF.1/INITIALISATION SFP			X	X											
FDP_ACF.1/SVD TRANSFER SFP						X									
FDP_ACF.1/PERSONALISATION SFP											X				
FDP_ACF.1/SIGNATURE CREATION SFP										X	X				
FDP_ACF.1/SCD IMPORT SFP													X		
FDP_ETC.1/SVD TRANSFER						X									
FDP_ITC.1/DTBS										X					
FDP_ITC.1/SCD													X		
FDP_RIP.1				X							X				
FDP_SDI.2/PERSISTENT				X	X						X	X			
FDP_SDI.2/DTBS										X					
FDP_UCT.1.1/RECEIVER													X		
FDP_UIT.1/SVD TRANSFER						X									
FDP_UIT.1/TOE DTBS										X					
FIA_AFL.1			X								X				
FIA_ATD.1			X								X				
FIA_UAU.1			X								X				
FIA_UID.1			X								X				
FMT_MOF.1/SIGN				X							X				
FMT_MOF.1/PATCH															X
FMT_MOF.1/CCLI														X	
FMT_MSA.1/ADMINISTRATOR			X	X											
FMT_MSA.1/SIGNATORY											X				
FMT_MSA.2											X		X		
FMT_MSA.3			X	X							X		X		

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

Table 3 – Functional Requirement to TOE Security Objective Mapping

7.3.2. Security Requirements Sufficiency

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

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

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

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive [15], storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1/Sign, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_FLS.1 tests the working conditions of the TOE and guarantees a secure state when integrity is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are

countered by FPT_FLS is differential fault analysis (DFA). The RNG failure would prevent critical protections of the IC to operate normally while handling the SCD and is also prevented by FPT_FLS.

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

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP.

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

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

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

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [15], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

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

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

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

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

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

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

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

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

OT.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FTP_ITC.1/SCD Import and FDP_UCT.1/Receiver that ensure that a trusted channel is provided and that confidentiality is maintained. Security functions specified by FDP_ACC.1/SCD Import SFP, FDP_ITC.1/SCD, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, and FDP_ACF.1/SCD Import SFP ensure that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions. Confidentiality is preserved with FCS_COP.1/ENC and integrity with FCS_COP.1/MAC.

Security function FCS_CKM.4 destroys the SCD before a SCD is re-imported into the TOE.

OT.CCLI_END (Secure termination of Card Content Loading and Installation) is provided by FMT_MOF.1/CCLI and FMT_SMF.1 which ensure that the access to the Card Content Loading and Installation is provided to the Administrator during phase 3.

OT.PATCH_END (Secure termination of Patching) is provided by FMT_MOF.1/Patch and FMT_SMF.1 which ensure that the access to the Patching mechanism termination is provided to the Administrator.

8. TOE summary specification

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation.

SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization and data communication required are satisfied.

SF.Administration

In Initialization Phase, this TSF provides Card initialization and pre-personalization services as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

This TSF also provides personalization functions to allow the Administrator to create and set the initial File System (LDS).

SF.Signatory Authentication

This TSF manages the identification and authentication of the Signatory and enforces role separation between the Signatory and the Administrator.

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 and SHA-1 hashing calculated by the host. The signature is calculated based on PKCS#1 version 1.5 [11].

SF.Secure Messaging

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

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).

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.

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, secure deallocation, card content loading and installation and patching services.

[More details disclosed upon request to support@athena-scs.com]

9. Terminology

Term	Definition
CC	Common Criteria
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).
DI	Dual Interface
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.
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.

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

10. References

[1] Common Criteria for Information Technology Security Evaluation — CCMB-2006-09-001 — Part 1: Introduction and general model, September 2006.

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

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

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

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

[6] STMicroelectronics 23YR80 Technical Datasheet – Revision 2

[7] STMicroelectronics 23YR48 Technical Datasheet – Revision 1

[8] BSI-PP-0035-2007 – Security IC Platform Protection Profile – version 1.0 – EAL4+

[9] Certification Report ANSSI-2012/68 – STMicroelectronics – 20 Dec 2012

[10] Sx23YRxx Security Target - Public Version – Ref: SMD_Sx23YRxx_ST_09_002 Rev 03.00 – STMicroelectronics – version 03.00

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

[12] 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]

[13] GlobalPlatform, Card Specification, Version 2.1.1, March 2003

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

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

[16] 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.

[17] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[18] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

[19] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[20] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[21] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[22] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[23] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography