COMMON CRITERIA SECURITY TARGET

IAS ECC - Secure Signature Creation Device - CC Ideal Citiz

Reference: ***SSE-0000087592***

Date: ***2011-10-13***

COMMON CRITERIA SECURITY TARGET

IAS ECC - SECURE SIGNATURE CREATION DEVICE - CC IDEAL CITIZ

TABLE OF CONTENTS

1 SECURITY TARGET INTRODUCTION 6
1.1 SECURITY TARGET AND TOE REFERENCE 6
1.2 GENERAL OVERVIEW OF THE TARGET OF EVALUATION (TOE) 6
1.2.1 Product presentation 6
1.2.2 TOE Type 7
1.2.3 Usage and major security features of the TOE 7
1.3 TOE DESCRIPTION 9
1.3.1 TOE boundary 9
1.3.2 TOE architecture 10
1.3.3 TOE life cycle 10

2 CC CONFORMANCE CLAIM 13
2.1 CONFORMANCE WITH THE COMMON CRITERIA 13
2.2 CONFORMANCE WITH AN ASSURANCE PACKAGE 13
2.3 CONFORMANCE WITH A PROTECTION PROFILE 13
2.3.1 Protection Profile reference 13
2.3.2 Protection Profile Refinements 14
2.3.3 Protection Profile addition 14
2.3.4 Protection Profile Claims rationale 15
2.4 CONFORMANCE WITH THE CC SUPPORTING DOCUMENTS 15
2.4.1 Application of Attack Potential to Smartcards 16
2.4.2 Composite product evaluation for Smartcards and similar devices 16

3 SECURITY PROBLEM DEFINITION 17
3.1 ASSETS 17
3.2 SUBJECTS 17
3.2.1 Subjects Definition 17
3.2.2 Threat agents 18
3.3 THREATS 18
3.4 ORGANISATIONAL SECURITY POLICIES 19
3.5 ASSUMPTIONS 20

4 SECURITY OBJECTIVES 21
4.1 SECURITY OBJECTIVES FOR THE TOE 21
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 23
4.3 SECURITY OBJECTIVES RATIONALE 24

4.3.1 Security Objectives Coverage 24
4.3.2 Security Objectives Sufficiency 25

5 EXTENDED COMPONENTS DEFINITION 30

6 SECURITY REQUIREMENTS 31

6.1 SECURITY FUNCTIONAL REQUIREMENTS 31
6.1.1 TOE Security Functional Requirements 31
6.1.2 Protection of the TSF (FPT) 44
6.1.3 Security Functional Requirements for the IT Environment 49
6.1.4 Security Functional Requirements for the Non-IT Environment 54
6.2 SECURITY ASSURANCE REQUIREMENTS 54
6.2.1 Rationale for Assurance Level 5 Augmented 55
6.2.2 Rationale for TOE assurance requirements conformance to PPs [R8] & [R9] 55
6.3 SECURITY REQUIREMENTS RATIONALE 57
6.3.1 Security Requirement Coverage 57
6.3.2 Security Requirements Sufficiency 59
6.3.3 Dependency Rationale 63
6.3.4 Security Requirements Grounding in Objectives 66

7 TOE SUMMARY SPECIFICATION 68

7.1 SECURITY FUNCTIONALITY DESCRIPTION 68
7.1.1 Chip security functionalities 68
7.1.2 Low level security functionalities 69
7.1.3 Operating system security functionalities 70
7.1.4 Application manager security functions 72
7.1.5 Application security functionalities 72
7.2 SECURITY FUNCTIONALITY RATIONALE 75

8 DEFINITIONS, GLOSSARY AND ACRONYMS 81

8.1 GLOSSARY 81
8.2 ACRONYMS 83

9 REFERENCE AND APPLICABLE DOCUMENTS 85

9.1 REFERENCE DOCUMENTS 85
9.2 APPLICABLE DOCUMENTS 87

List of figures

Figure 1: Structural view of the SSCD 9

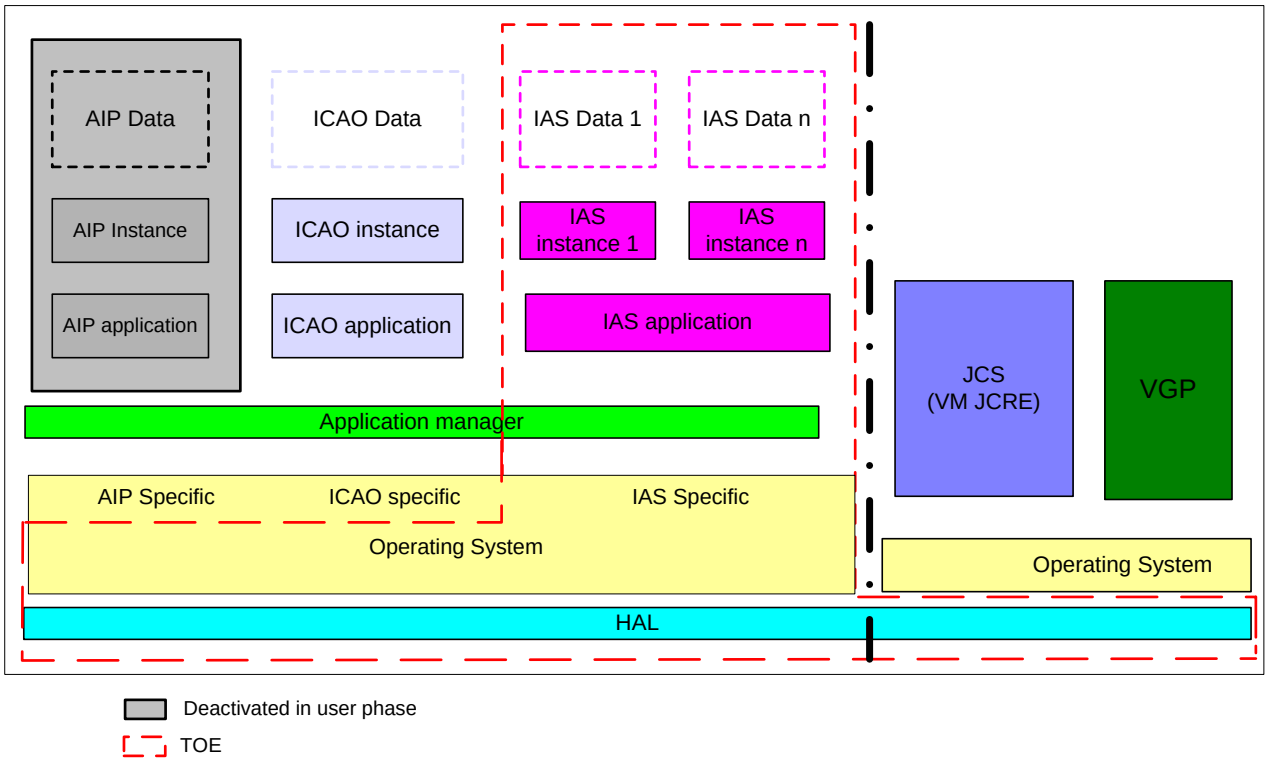

Figure 2: Architecture of the CC Ideal Citiz..... 10
Figure 3: TOE life cycle..... 12

1 SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET AND TOE REFERENCE

ST reference:

Title	:	IAS ECC - SECURE SIGNATURE CREATION DEVICE - CC IDEAL CITIZ
Version	:	-
Security target identifier	:	SSE-0000087592

TOE reference:

Chip identifier	:	SB23YR80 Version B and SB23YR48 Version B
Masked chip reference	:	SB23YR48 SAI and SB23YR80 SAI
Crypto library		NesLib Version 3.0
Assurance Level		EAL 6+, augmented with ALC_FLR.1
TOE Identifier		IDEAL/SB23YR80/YR48/1.6.0
Administration guidance	:	0000064845-01 - IDEAL - AGD - IAS ECC PERSONALIZATION GUIDANCE
User guidance	:	0000065958-01 - IDeal - AGD - IAS ECC Operational user guidance

CC compliance:

Version	:	3.1
Assurance level	:	EAL5+ augmented with ALC_DVS.2 and AVA_VAN.5.
Chip certificate reference	:	ANSSI-2010/02
Protection Profile	:	PP SSCD Type 2 [R8] and Type 3 [R9]

1.2 GENERAL OVERVIEW OF THE TARGET OF EVALUATION (TOE)

1.2.1 Product presentation

The CC IDeal Citiz product is the DUAL integrated circuit chip embedding

- An Operating system providing:
  - Java Card v2.2.2 interfaces, as specified in [R28]
  - Extended interfaces for targeted applications needs
- A Set of applications
  - An IAS ECC application compliant with **[R31]**,
  - An ICAO application compliant with **[R18]** and
  - An AIP Application, compliant with, [R32]which performs the pre-personalization and the personalization operations of IAS and ICAO applications (this application is not accessible once in Operational Use phase).

- A card manager application compliant with the [25] standard. This application enables the card issuer to add functionality to the product by loading and executing new applets, even in the evaluated configuration. This functionality is out of the scope of the evaluation.

The evaluated IAS and ICAO applications are protected against post issuance Java Card applet loading and execution thanks to a firewall mechanism.

The evaluated Operating system and IAS application are supporting the fingerprint Match On Card (MOC) algorithm. The MOC algorithm is active on the product, and the MOC can be used as a signatory PIN.

The BAC and EAC are out of the scope of the current ST but will be evaluated in others ST,

1.2.2 TOE Type

This security target specifies the functional and security assurance requirements applicable to the CC IDeal Citiz smart card. The CC IDeal Citiz is comprised of embedded software masked on a referenced IC and its cryptographic library.

The IC and the cryptographic library have been evaluated separately. The TOE evaluation is thus a composite evaluation of an embedded software on a certified IC with its cryptographic library.

The IAS application provides services responding to the new needs of the electronic administration (e-administration). In its operating environment, the IAS application especially offers electronic signature services, responding to the characteristics of a Secure Signature Creation Device (SSCD), in compliance with the European directive [R13]:

- Generation of an electronic signature key pair;
- Destruction of the electronic signature key pair;
- Loading of electronic signature private key;
- Electronic signature creation.

Note: as the card is a DUAL interface card, the IAS application provides its services over the contact and the contact less interface.

1.2.3 Usage and major security features of the TOE

The TOE is a secure signature-creation device (SSCD Type 2 and SSCD 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 [R13]. The destruction of the SCD is mandatory before the TOE loads or generates a new pair SCD/SVD.

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

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

2) to create qualified electronic signatures:

    a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment

    b) using appropriate hash functions that are, according to **[R14]**, agreed as suitable for qualified electronic signatures

    c) after appropriate authentication of the signatory by the TOE.

    d) using appropriate cryptographic signature function that employs appropriate cryptographic parameters agreed as suitable according to **[R14]**.

Signature generation by means of a SSCD Type 2 TOE requires that the SCD/SVD pair has been generated by and imported from a SSCD Type 1. Consequently, there is an interdependence where a SSCD Type 1 constitutes the environment of the TOE.

The TOE implements all IT security functionalities 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. To this end, the TOE may implement IT measures to support a trusted path to a trusted human interface device.

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) import of the SCD or generating a SCD/SVD pair,

2) personalisation 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 implementing a human interface for user authentication by a trusted human interface device connected via a trusted channel with the TOE.

Figure 1 shows the structural perspective of the TOE and its environment. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE. They shall communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively.

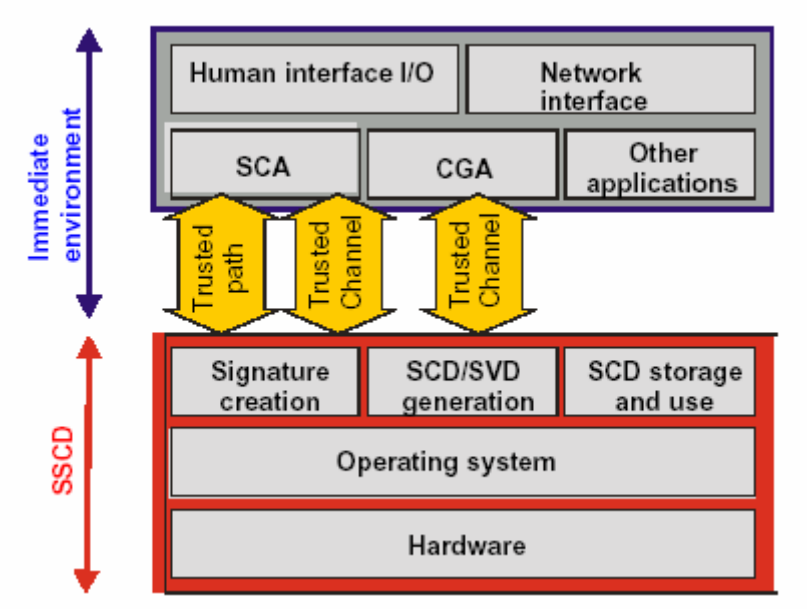

Figure 1: Structural view of the SSCD

Application note 1: 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. This ST may as well be applied to environments where the certificates expressed as 'qualified certificates' in this ST do not fulfil the requirements laid down in Annex I and Annex II of the Directive **[R13]**.

With this respect the notion of qualified certificates in this ST refers to the fact that 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 **[R13]**, article 5, paragraph 1. As a consequence, this standard does not prevent a device itself from being regarded as a SSCD, even when used together with a non-qualified certificate.

1.3 TOE DESCRIPTION

1.3.1 TOE boundary

The Target Of Evaluation (TOE) is a DUAL (contact & contactless) integrated circuit chip.

The TOE boundary encompasses:

- The Operating System
- The IAS application
- The ST embedded crypto library: NesLib Version 3.0

- The ST chip: SB23YR80 Version B and SB23YR80 Version B

1.3.2 TOE architecture

The TOE is embedding:

– the IAS application, which meets all the needs of the electronic administration and is compliant with **[R31]**. The IAS application may be instantiated several times,

The TOE allows any additional applets loading during its operational use.

The architecture of the CC IDeal Citiz is given in:

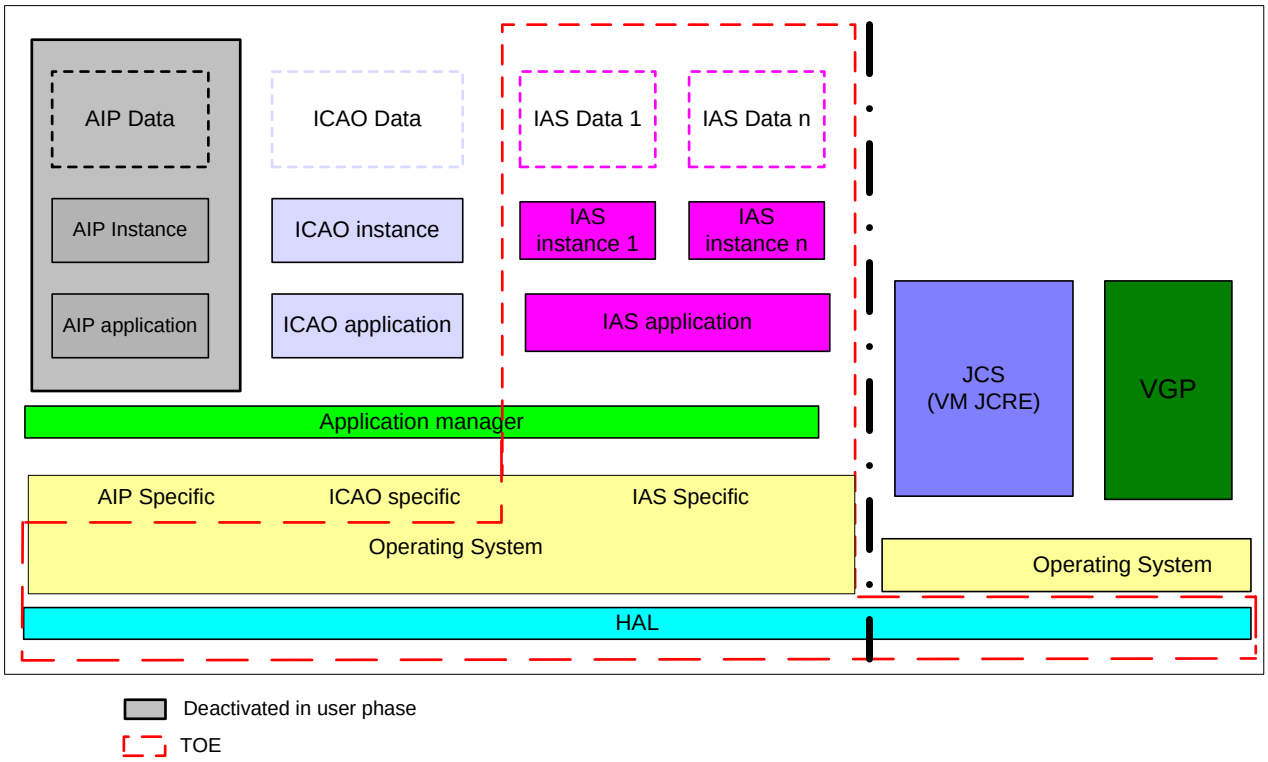

Figure 2: Architecture of the CC Ideal Citiz

1.3.3 TOE life cycle

The TOE is a smart card, whose life cycle may be divided into 7 phases:

Phase 1 Development of the smart card embedded software

Morpho is in charge of the development of the smart card integrated software and of the specification requirements for the initialisation of the integrated circuit.

Phase 2 Integrated Circuit (IC) Development

STMicroelectronics designs the IC, develops the dedicated software IC and transmits the information, the software and the tools to the developer's embedded software (Morpho), by protected verification and delivery procedures. From the integrated circuit, the dedicated software and the embedded software, they build the integrated circuit smart card data base, indispensable for creating the integrated circuit mask.

Phase 3 Manufacture and test of the integrated circuit

STMicroelectronics is in charge of the production of the integrated circuit which occurs in three principal steps: manufacture, test and initialisation of the integrated circuit.

Phase 4 Encapsulation and test of the integrated circuit

The integrated circuit packaging manufacturer in charge of packaging (encapsulation) and testing of the integrated circuit.

Phase 5 Smart card product Finish

The smart card manufacturer in charge of finishing and testing the smart card.

Phase 6 Smart card personalisation

The personaliser is in charge of personalising the smart card and performing final tests.

Phase 7 Smart card use

The smart card issuer is in charge of product delivery to the end user, as well as for the end of the life cycle.

The TOE life cycle as a SSCD is shown below. Basically, it consists of a development phase and the operational phase. This document refers to the operational phase which starts with personalisation including SCD/SVD generation and SCD import if necessary. This phase represents installation, generation, and start-up in the CC terminology. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use). The life cycle ends with the destruction of the SSCD.

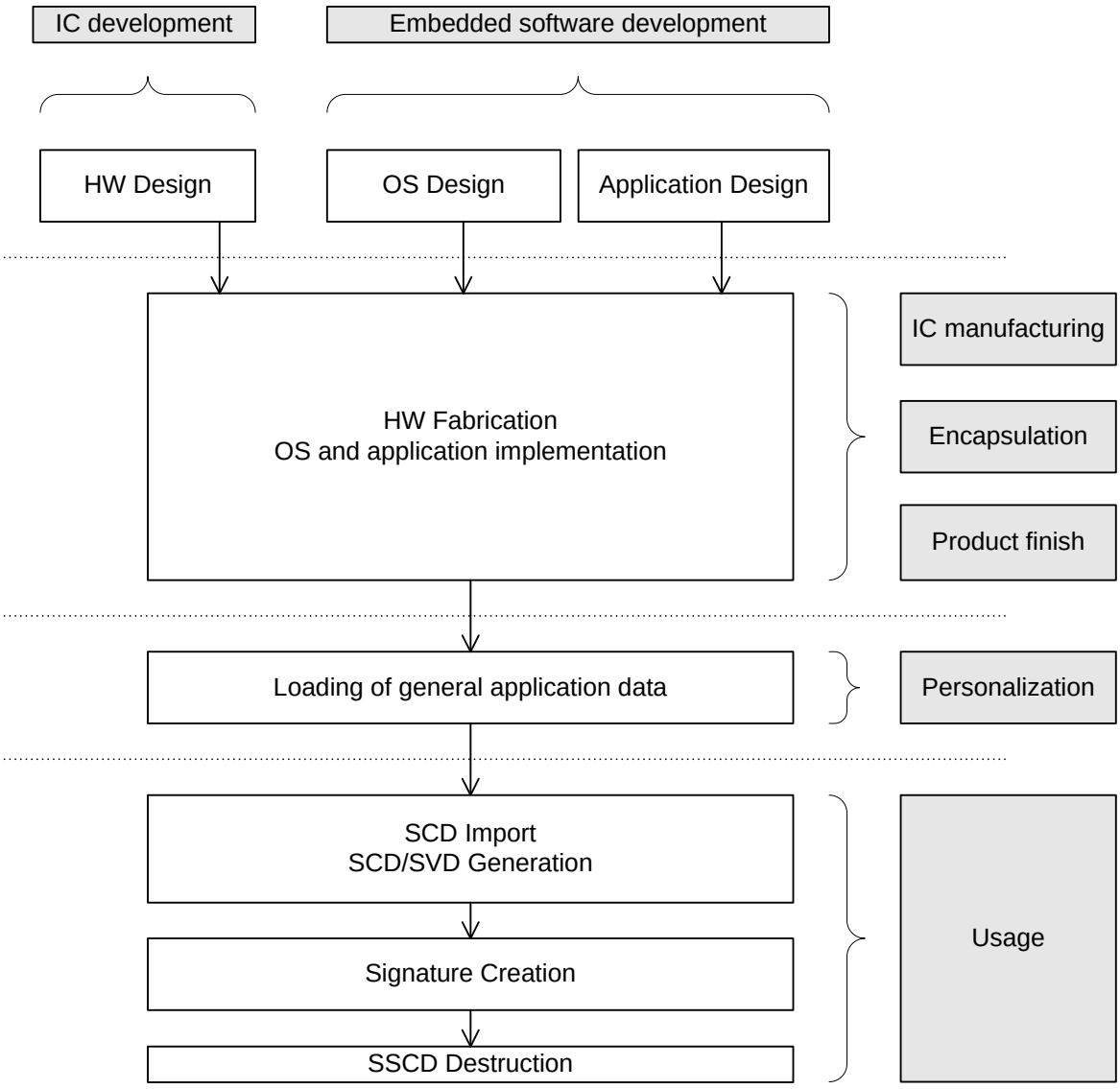

Figure 3: TOE life cycle

If a patch is necessary, it will be developed under the same conditions as the whole embedded software and will be included in the chip during manufacturing (phase 3 of the smart card life cycle) or during pre-personalization (phase 5 of the smart card life cycle).

2 CC CONFORMANCE CLAIM

2.1 CONFORMANCE WITH THE COMMON CRITERIA

This Security Target is compliant with Common Criteria v3.1 [R5], [R6]:

- Part 1 of the Common Criteria, Version 3.1, Release 3, dated July 2009 (see [R4])
- Part 2 of the Common Criteria, Version 3.1, Release 3, dated July 2009 (see [R5]),
- Part 3 of the Common Criteria, Version 3.1, Release 3, dated July 2009 (see [R6]),

as follows

- Part 2 extended,
- Part 3 conformant.

2.2 CONFORMANCE WITH AN ASSURANCE PACKAGE

The assurance level specified in the present security target and in its documentation is EAL 5 augmented by the following components defined in CC part 3 [R6]:

– ALC_DVS.2,
– AVA_VAN.5.

2.3 CONFORMANCE WITH A PROTECTION PROFILE

2.3.1 Protection Profile reference

This Security Target is compliant with the SSCD Type 2 and SSCD Type 3 Protection Profiles [R8] & [R9].

However, as those PPs [R8] & [R9] are compliant with CC v2.1 [R1], [R2], [R3] and this ST is compliant with CC v3.1 [R4], [R5], [R6], some requirements from the PPs [R8] & [R9] have been updated to match CC v3.1 [R4], [R5], [R6]. A rationale on how the modified requirements still fulfil the PPs [R8] & [R9] requirements is given in §2.3.4 and §6.2.2.

Therefore this Security Target claims conformance to the PPs [R8] & [R9]:

– Protection Profile - Secure Signature-Creation Device Type 2 – Ref. PP0005, Version 1.04, 25 July 2001
– Protection Profile - Secure Signature-Creation Device Type 3 – Ref. PP0006, Version 1.05, 25 July 2001

Those PPs [R8] & [R9] are established by CEN/ISSS for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic

signatures **[R13]**, as generally recognised standard for electronic-signature products in the Official Journal of the European Community.

The intent of those PPs [R8] & [R9] is to specify functional and assurance requirements defined in the Directive **[R13]**, Annex III for secure signature-creation devices (SSCD) which is the target of evaluation (TOE). Member States shall presume that there is compliance with the requirements laid down in Annex III of the Directive **[R13]** when an electronic signature product is evaluated to a Security Target (ST) that is compliant with one or both of those PPs [R8] & [R9].

Those PPs [R8] & [R9] define the security requirements of a SSCD for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. The TOE may implement additional functions and security requirements e.g. for editing and displaying the data to be signed (DTBS), but these additional functions and security requirements are not subject of those PPs [R8] & [R9].

2.3.2 Protection Profile Refinements

No specific refinement was performed to the Protection Profile [R8] & [R9].

2.3.3 Protection Profile addition

The following threats are considered in addition to the threats listed in the PP ([R8] & [R9]):

- T.Tracking
- T.Skimming
- T.Listening

These additional threats are marked in italics in this ST.

The following objective is considered in addition to the objectives listed in the PPs ([R8] & [R9]):

- O.Privacy

This additional objective is marked in italics in this ST.

The following requirements are considered in addition to the requirements listed in the PPs ([R8] & [R9]):

- FCS_COP.1/TDES (to cover the secure messaging)
- FCS_COP.1/MAC (to cover the secure messaging)

Additional requirements are marked in italics in this ST.

The assignments of the following requirements have been augmented compared to those of the PPs [R8] & [R9]**,** in order to cover the protection for communication in contactless mode:

- FIA_UID.1
- FIA_UAU.1

Augmentations are marked in italics inside the SFRs.

2.3.4 Protection Profile Claims rationale

As the PPs SSCD [R8] & [R9] are compliant with CC v2.1, there is no specification about the type of conformance required (strict or demonstrable). Therefore, the goal of this Security Target is to be conformant to the PPs [R8] & [R9] in the sense of CC v2.

The differences between this Security Target security objectives and requirements and those of the PPs SSCD [R8] & [R9]**,** to which conformance is claimed, have been identified and justified in each impacted chapter. They have been recalled in the previous section.

The TOE type defined in this security target is exactly the same than the one defined in the PPs [R8] & [R9]: an IC with embedded software, and the SSCD application conformant to the European directive **[R13]**.

In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the PPs SSCD [R8] & [R9].

The security problem definition presented in chapter 3 clearly shows the additions to the security problem statement of the PPs.

The security objectives rationale presented in chapter 4.3 clearly identifies modifications and additions made to the rationale presented in the PPs SSCD [R8] & [R9].

Similarly, the security requirements rationale presented in chapter 6.3 has been updated with respect to the protection profile.

All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the present document.

Some assignments operations in the SFRs are determined in the PPs [R8] & [R9], some are left with unspecified values. Assignments made by the PPs [R8] & [R9] authors are marked as bold text, while assignments made by the ST author are marked as bold text and in italics.

2.4 CONFORMANCE WITH THE CC SUPPORTING DOCUMENTS

This security target address a smartcard TOE and therefore, the associated evaluation shall be performed in compliance with all CC mandatory supporting documents related to smartcard evaluations:

2.4.1 Application of Attack Potential to Smartcards

This document **[R20]** shall be used instead of the CEM [R7] when calculating the attack potential of the successful attack performed during AVA_VAN analysis. This document impacts only the vulnerability analysis performed by the ITSEF, and is not detailed here.

2.4.2 Composite product evaluation for Smartcards and similar devices

This document **[R21]** shall be used in addition to the CC part 3 [R6] and to the CEM [R7]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF when performing a “composite evaluation”. This is the case for the current TOE as the underlying IC SB23YR80 Version B (or SB23YR80 Version B) is already evaluated and certified under the reference: ANSSI-2010/02. Therefore, the following additional assurance requirements apply for this TOE:

- ASE_COMP.1 for the security target ;
- ALC_COMP.1 for the life cycle support ;
- ADV_COMP.1 for the development activity ;
- ATE_COMP.1 for the tests activity ;
- AVA_COMP.1 for the vulnerability assessment.

The statement of compatibility required by ASE_COMP additional requirements can be found in this security target, chapter 8.

3 SECURITY PROBLEM DEFINITION

3.1 ASSETS

SCD

Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).

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).

DTBS and DTBS-representation

Set of data, or its representation which is intended to be signed (Their integrity must be maintained).

VAD

PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)

RAD

Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained).

Signature-creation function of the SSCD using the SCD

The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures.

Electronic signature

Unforgeability of electronic signatures must be assured.

3.2 SUBJECTS

3.2.1 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 initialisation, TOE personalisation or other TOE administrative functions.

S.Signatory
User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.

3.2.2 Threat agents

S.OFFCARD

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

3.3 THREATS

TOE threats	PP SSCD Type 2 threats	PP SSCD Type 3 threats	Additional threats
T.Hack_Phys	T.Hack_Phys	T.Hack_Phys	
T.SCD_Divulg	T.SCD_Divulg	T.SCD_Divulg	
T.SCD_Derive	T.SCD_Derive	T.SCD_Derive	
T.Sig_Forgery	T.Sig_Forgery	T.Sig_Forgery	
T.Sig_Repud	T.Sig_Repud	T.Sig_Repud	
T.SVD_Forgery	T.SVD_Forgery	T.SVD_Forgery	
T.DTBS_Forgery	T.DTBS_Forgery	T.DTBS_Forgery	
T.SigF_Misuse	T.SigF_Misuse	T.SigF_Misuse	
T.Tracking			*T.Tracking*
T.Skimming			*T.Skimming*
T.Listening			*T.Listening*

T.Hack_Phys Physical attacks through the TOE interfaces

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

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

An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive Derive the signature-creation data

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

T.Sig_Forgery Forgery of the electronic signature

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

T.Sig_Repud Repudiation of signatures

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

T.SVD_Forgery Forgery of the signature-verification data

An attacker forges the SVD presented by the TOE. This result 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 intends 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.Tracking Remote tracking of the TOE

An attacker tries to trace the movement of the TOE by identifying remotely the TOE by establishing or listening a communication through the contactless communication interface.

T.Skimming Remote unauthorized disclosure of TOE data

An attacker tries to read parts of data stored in the TOE via the contactless interface.

T.Listening Listening of contactless communications

An attacker listens exchanges between the TOE and an authorized terminal communicating using the contactless interface in order to get the exchanged data.

3.4 ORGANISATIONAL SECURITY POLICIES

TOE OSP	PP SSCD Type 2 OSP	PP SSCD Type 3 OSP
P.CSP_QCERT	P.CSP_QCERT	P.CSP_Qcert
P.QSign	P.QSign	P.QSign
P.Sigy_SSCD	P.Sigy_SSCD	P.Sigy_SSCD

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 alia 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 and is created by a SSCD.

P.Sigy_SSCD TOE as secure signature-creation device

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

3.5 ASSUMPTIONS

TOE assumptions	PP SSCD Type 2 assumptions	PP SSCD Type 3 assumptions
A.CGA	A.CGA	A.CGA
A.SCA	A.SCA	A.SCA
A.SCD_Generate	A.SCD_Generate	

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

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

4 SECURITY OBJECTIVES

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

4.1 SECURITY OBJECTIVES FOR THE TOE

TOE objectives	PP SSCD Type 2 objectives	PP SSCD Type 3 objectives	Additional objectives
OT.EMSEC_DESIGN	OT.EMSEC_DESIGN	OT.EMSEC_DESIGN	
OT.LIFECYCLE_SECURITY	OT.LIFECYCLE_SECURITY	OT.LIFECYCLE_SECURITY	
OT.SCD_SECRECY	OT.SCD_SECRECY	OT.SCD_Secrecy	
OT.SCD_SVD_Corresp	OT.SCD_SVD_Corresp	OT.SCD_SVD_Corresp	
OT.SVD_Auth_TOE	OT.SVD_Auth_TOE	OT.SVD_Auth_TOE	
OT.Tamper_ID	OT.Tamper_ID	OT.Tamper_ID	
OT.Tamper_Resistance	OT.Tamper_Resistance	OT.Tamper_Resistance	
OT.SCD_Transfer	OT.SCD_Transfer		
OT.Init		OT.Init	
OT.SCD_Unique		OT.SCD_Unique	
OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE	
OT.Sigy_SigF	OT.Sigy_SigF	OT.Sigy_SigF	
OT.Sig_Secure	OT.Sig_Secure	OT.Sig_Secure	
O.Privacy			*O.Privacy*

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 initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import and in case of re-generation.

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

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

OT.SCD_SVD_Corresp **Correspondence between SVD and SCD**

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify 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_Transfer **Secure transfer of SCD between SSCD**

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

OT.Init **SCD/SVD generation**

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

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

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

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

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

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

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

OT.Sig_Secure **Cryptographic security of the electronic signature**

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

O.Privacy ***Protection of TOE identification and of stored data***

During the TOE operational use phase, when communicating using the contactless interface, the TOE shall disclose identification data or data stored on the card only to a successfully authenticated terminal through a communication channel that protects data from disclosure to an unauthorized third party.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

TOE objectives for the environment	PP SSCD Type 2 objectives for the environment	PP SSCD Type 3 objectives for the environment
OE.SCD_SVD_CORRESP	OE.SCD_SVD_CORRESP	
OE.SCD_TRANSFER	OE.SCD_TRANSFER	
OE.SCD_UNIQUE	OE.SCD_UNIQUE	
OE.CGA_QCERT	OE.CGA_QCERT	OE.CGA_QCERT
OE.SVD_AUTH_CGA	OE.SVD_AUTH_CGA	OE.SVD_AUTH_CGA
OE.HI_VAD	OE.HI_VAD	OE.HI_VAD
OE.SCA_Data_Intend	OE.SCA_Data_Intend	OE.SCA_Data_Intend

OE.SCD_SVD_Corresp Correspondence between SVD and SCD

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

OE.SCD_Transfer Secure transfer of SCD between SSCD

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

OE.SCD_Unique Uniqueness of the signature-creation data

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible low.

OE.CGA_Qcert Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA CGA verifies the authenticity of the SVD

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

OE.HI_VAD Protection of the VAD

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

OE.SCA_Data_Intend Data intended to be signed

The SCA

- 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,
- sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE
- attaches the signature produced by the TOE to the data or provides it separately.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Security Objectives Coverage

Table 4-1 provides the mapping of the security objectives for the TOE.

	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Transfer	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Init	OT.SCD_Unique	*OT.Privacy*	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend
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

	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Transfer	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Init	OT.SCD_Unique	*OT.Privacy*	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique	OE.CGA_Qcert	OE.SVD_Auth_CGA	OE.HI_VAD	OE.SCA_Data_Intend
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		X
T.Tracking														X							
T.Skimming														X							
T.Listening														X							
A.SCD_Generate															X	X	X				
A.CGA																		X	X		
A.SCA																					X
P.CSP_Qcert					X										X			X			
P.QSign										X	X							X			X
P.Sigy_SSCD										X		X	X				X				

Table 4-1: Security Environment to Security Objectives Mapping

4.3.2 Security Objectives Sufficiency

4.3.2.1 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 **[R13]**, article 5, paragraph 1. Directive **[R13]**, 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 OE.SCD_Unique (if SCD is imported) or OT.SCD_Unique (if SCD/SVD pair is generated) 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.

4.3.2.2 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 and 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 **[R13]**, 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 ensure 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 OE.SCD_Unique (if SCD is imported) or by OT.SCD_Unique (if SCD/SVD pair is generated) that provides cryptographic secure generation of the SCD/SVD-pair. OT.Sig_Secure ensures cryptographic secure electronic signatures.

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then 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 **[R13]**, 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), OE_SCD_Unique or OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Transfer (Secure transfer of SCD between SSCD), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity). OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OE_SCD_Unique or 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.

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.Tracking (Remote tracking of the TOE) is met by O.Privacy, as O.Privacy does not allow the TOE to identify itself to an unknown terminal, therefore an attacker will not be able to identify and track a dedicated TOE.

T.Skimming (Remote unauthorized disclosure of TOE data) is met by O.Privacy because O.Privacy forbids to disclose data stored on the TOE to an unauthorized terminal, therefore an attacker will not be able to access to data stored on the TOE.

T.Listening (Listening of contactless communications) is met by O. Privacy because O.Privacy protects data exchanged between the TOE and an authorized terminal from disclosure to an unauthorized third party.

4.3.2.3 ASSUMPTIONS AND SECURITY OBJECTIVE SUFFICIENCY

A.SCD_Generate (Trustworthy SCD/SVD generation) establishes a trustworthy SCD/SVD pair. This requires 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.

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

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

and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

5 EXTENDED COMPONENTS DEFINITION

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on 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.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling: FPT_EMSEC TOE Emanation ---------- 1

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 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 action defined to be auditable.

FPT_EMSEC.1 TOE Emanation

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]**.

Hierarchical to: No other components.

Dependencies: No other components.

6 SECURITY REQUIREMENTS

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

Security functional requirements components given in section 6.1.1, excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [R5]. Some security functional requirements represent extensions to [R5].

Operations for assignment, selection and refinement have been made. Some operations in the SFRs are determined in the PPs [R8] & [R9], some are let with unspecified values. Assignments made by the PPs [R8] & [R9] authors are marked as bold text, while assignments made by the ST author are marked as bold text and in italics.

The TOE security assurance requirements statement given in section 6.2 is drawn from the security assurance components from Common Criteria part 3 [R6].

Section 6.1.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 6.1.4.

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 TOE Security Functional Requirements

TOE SFR	PP SSCD type 2 SFR	PP SSCD type 3 SFR	Additional SFR
Cryptographic support			
FCS_CKM.1		FCS_CKM.1	
FCS_CKM.4	FCS_CKM.4	FCS_CKM.4	
FCS_COP.1	FCS_COP.1	FCS_COP.1	*FCS_COP.1*
USER DATA PROTECTION			
FDP_ACC.1	FDP_ACC.1	FDP_ACC.1	
FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	
FDP_ETC.1	FDP_ETC.1	FDP_ETC.1	
FDP_ITC.1	FDP_ITC.1	FDP_ITC.1	
FDP_RIP.1	FDP_RIP.1	FDP_RIP.1	
FDP_SDI.2	FDP_SDI.2	FDP_SDI.2	
FDP_UCT.1	FDP_UCT.1		
FDP_UIT.1	FDP_UIT.1	FDP_UIT.1	
IDENTIFICATION AND AUTHENTICATION			

TOE SFR	PP SSCD type 2 SFR	PP SSCD type 3 SFR	Additional SFR
FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	
FIA_ATD.1	FIA_ATD.1	FIA_ATD.1	
FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	*FIA_UAU.1*
FIA_UID.1	FIA_UID.1	FIA_UID.1	*FIA_UID.1*
SECURITY MANAGEMENT			
FMT_MOF.1	FMT_MOF.1	FMT_MOF.1	
FMT_MSA.1	FMT_MSA.1	FMT_MSA.1	
FMT_MSA.2	FMT_MSA.2	FMT_MSA.2	
FMT_MSA.3	FMT_MSA.3	FMT_MSA.3	
FMT_MTD.1	FMT_MTD.1	FMT_MTD.1	
FMT_SMR.1	FMT_SMR.1	FMT_SMR.1	
Protection of the TSF			
	FPT_AMT.1	FPT_AMT.1	
FPT_EMSEC.1	FPT_EMSEC.1	FPT_EMSEC.1	
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1	
FPT_PHP.1	FPT_PHP.1	FPT_PHP.1	
FPT_PHP.3	FPT_PHP.3	FPT_PHP.3	
FPT_TST.1	FPT_TST.1	FPT_TST.1	
TRUSTED PATHS/CHANNELS			
FTP_ITC.1	FTP_ITC.1	FTP_ITC.1	
FTP_TRP.1	FTP_TRP.1	FTP_TRP.1	

FPT_AMT.1 is removed according to Common Criteria 3.1 R2 [R4]**.**

6.1.1.1 CRYPTOGRAPHIC SUPPORT (FCS)

6.1.1.1.1 CRYPTOGRAPHIC KEY GENERATION (FCS_CKM.1)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **List of approved algorithms and parameters**.

Assignment	Cryptographic key generation algorithm: **[R15]**, **[R16]**, [R19] Cryptographic key sizes: ***1024, 1280, 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits for RSA, and 192, 224, 256, 384 and 521 for Elliptic curves***

6.1.1.1.2 CRYPTOGRAPHIC KEY DESTRUCTION (FCS_CKM.4)

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in case of re-importation of the SCD in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.
Assignment	Cryptographic key destruction method: ***Key overwriting*** List of standards: ***None***

Application note 2: The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD is re-imported into the TOE. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE.

6.1.1.1.3 CRYPTOGRAPHIC OPERATION (FCS_COP.1)

FCS_COP.1/CORRESP Cryptographic operation

FCS_COP.1.1 / CORRESP	The TSF shall perform **SCD / SVD correspondence verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **List of approved algorithms and parameters**.
Assignments	Cryptographic algorithms: ❑ ***RSASSA PKCS1-v1_5 SHA-1*** *[R22]* ❑ ***RSASSA PKCS1-v1_5 SHA-256*** *[R22]* ❑ ***ISO15946 ECDSA*** Cryptographic key sizes: ***1024, 1280, 1536, 1792, 2048, 2560 or 3072 bits for RSA, and 192, 224, 256, 384 and 521 for Elliptic curves***

FCS_COP.1/SIGNING Cryptographic operation

FCS_COP.1.1 /	The TSF shall perform **digital signature-generation** in accordance with a

SIGNING	specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **List of approved algorithms and parameters**.
Assignments	Cryptographic algorithms: ❑ ***RSASSA PKCS1-v1_5 SHA-1*** *[R22]* ❑ ***RSASSA PKCS1-v1_5 SHA-256*** *[R22]* ❑ ***ISO15946 ECDSA*** Cryptographic key sizes: ***1024, 1280, 1536, 1792 or 2048, 2560 or 3072 bits for RSA, and 192, 224, 256, 384 and 521 for Elliptic curves***

FCS_COP.1/TDES ***Cryptographic operation – Encryption / Decryption Triple DES***

FCS_COP.1.1 / TDES	The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.
Assignment	List of cryptographic operations: ***secure messaging – encryption and decryption*** Cryptographic algorithm: ***Triple-DES in CBC mode*** Cryptographic key sizes: ***112 bits*** List of standards: ***ANSI X9.52***

FCS_COP.1/MAC ***Cryptographic operation – Retail MAC***

FCS_COP.1.1 / MAC	The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.
Assignment	List of cryptographic operations: ***secure messaging – message authentication code*** Cryptographic algorithm: ***Retail MAC*** Cryptographic key sizes: ***112 bits*** List of standards: ***ISO 9797 (MAC algorithm 3, block cipher DES,***

	Sequence Message Counter, padding mode 2)

6.1.1.2 USER DATA PROTECTION (FDP)

6.1.1.2.1 SUBSET ACCESS CONTROL (FDP_ACC.1)

FDP_ACC.1/SVD Transfer SFP **Subset access control**

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 3: FDP_ACC.1/SVD Transfer SFP will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

FDP_ACC.1/SCD Import SFP **Subset access control**

FDP_ACC.1.1 / SCD Import SFP	The TSF shall enforce the **SCD Import SFP** on **import of SCD by User**.

FDP_ACC.1/Personalisation SFP **Subset access control**

FDP_ACC.1.1 / Personalisation SFP	The TSF shall enforce the **Personalisation SFP** on **creation of RAD by Administrator**.

FDP_ACC.1/Signature-creation SFP **Subset access control**

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.**

FDP_ACC.1/Initialisation SFP **Subset access control**

FDP_ACC.1.1 / Initialisation SFP	The TSF shall enforce the **Initialisation SFP** on **generation of SCD/SVD pair by User**.

6.1.1.2.2 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

Initialisation attribute group		
User	SCD / SVD management	authorised, not authorised
SCD	secure SCD import allowed	no, yes
Signature-creation attribute group		
SCD	SCD operational	no, yes
DTBS	sent by an authorised SCA	no, yes

FDP_ACF.1/SVD Transfer SFP **Security attribute based access control**

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

Application note 4: FDP_ACF.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_ACF.1/SCD Import SFP **Security attribute based access control**

FDP_ACF.1.1 / SCD Import SFP	The TSF shall enforce the **SCD Import SFP** to objects based on **General attribute** and **Initialisation attribute group**.
FDP_ACF.1.2 / SCD Import SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes"**.
FDP_ACF.1.3 / SCD Import SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 / SCD Import SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **(a) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".** **(b) The user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".**

FDP_ACF.1/Personalisation SFP Security attribute based access control

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

FDP_ACF.1/Signature-creation SFP Security attribute based access control

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

FDP_ACF.1.3 / Signature-creation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4 / Signature-creation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **(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".**

FDP_ACF.1/Initialisation SFP Security attribute based access control

FDP_ACF.1.1 / Initialisation SFP	The TSF shall enforce the **Initialisation SFP** to objects based on **General attribute and Initialisation attribute**.
FDP_ACF.1.2 / Initialisation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "authorised" is allowed to generate SCD/SVD pair.**
FDP_ACF.1.3 / Initialisation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4 / Initialisation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: **The user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.**

6.1.1.2.3 EXPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES (FDP_ETC.1)

FDP_ETC.1/SVD Transfer Export of user data without security attributes

FDP_ETC.1.1 / SVD Transfer	The TSF shall enforce the **SVD Transfer** when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2 / SVD Transfer	The TSF shall export the user data without the user data's associated security attributes.

Application note 5: FDP_ETC.1/SVD Transfer SFP will be required only, if the TOE holds the SVD and the SVD is exported to the CGA for certification.

6.1.1.2.4 IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES (FDP_ITC.1)

FDP_ITC.1/SCD Import of user data without security attributes

FDP_ITC.1.1 / SCD	The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2 / SCD	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3 / SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **SCD shall be sent by an authorised SSCD**.

Application note 6: A SSCD of Type 1 is authorised to send SCD to a 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 are able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.

FDP_ITC.1/DTBS Import of user data without security attributes

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.1.3 / 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 7: A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

6.1.1.2.5 SUBSET RESIDUAL INFORMATION PROTECTION (FDP_RIP.1)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the **de-allocation of the resource from** the following objects: **SCD, VAD, RAD**.

6.1.1.2.6 STORED DATA INTEGRITY MONITORING AND ACTION (FDP_SDI.2)

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

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

FDP_SDI.2/Persistent Stored data integrity monitoring and action

FDP_SDI.2.1 / Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked persistent stored data**.
FDP_SDI.2.2 / Persistent	Upon detection of a data integrity error, the TSF shall **1. prohibit the use of the altered data** **2. inform the Signatory about integrity error**.

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

FDP_SDI.2/DTBS Stored data integrity monitoring and action

FDP_SDI.2.1 / DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.
FDP_SDI.2.2 / DTBS	Upon detection of a data integrity error, the TSF shall **1. prohibit the use of the altered data** **2. inform the Signatory about integrity error**.

6.1.1.2.7 BASIC DATA EXCHANGE CONFIDENTIALITY (FDP_UCT.1)

FDP_UCT.1/Receiver Basic data exchange confidentiality

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

6.1.1.2.8 DATA EXCHANGE INTEGRITY (FDP_UIT.1)

SVD Transfer SFP will be required only if the TOE holds the SVD and the SVD is exported to the CGA for certification.

FDP_UIT.1/SVD Transfer Data exchange integrity

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/TOE DTBS Data exchange integrity

FDP_UIT.1.1 / TOE DTBS	The TSF shall enforce the **Signature-creation SFP** to be able to **receive** the DTBS-representation in a manner protected from **modification, deletion and insertion** errors.
FDP_UIT.1.2 / TOE DTBS	The TSF shall be able to determine on receipt of user data, whether **modification, deletion and insertion** has occurred.

6.1.1.3 IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.1.3.1 AUTHENTICATION FAILURE HANDLING (FIA_AFL.1)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when [assignment: number] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **block RAD**.
Assignment	Number: ***3***

6.1.1.3.2 USER ATTRIBUTE DEFINITION (FIA_ATD.1)

FIA_ATD.1 User attribute definition

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

6.1.1.3.3 TIMING OF AUTHENTICATION (FIA_UAU.1)

FIA_UAU.1 Timing of authentication

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 channel 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.** **5. *Establishing a trusted channel with an authorized terminal through the contactless interface*** 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 8: “Local user” mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SGA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP_TRP.1/TOE.

6.1.1.3.4 TIMING OF IDENTIFICATION (FIA_UID.1)

FIA_UID.1 Timing of identification

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** ***4. Establishing a trusted channel with an authorized terminal***

	through the contactless interface on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.1.4 SECURITY MANAGEMENT (FMT)

6.1.1.4.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR (FMT_MOF.1)

FMT_MOF.1 Management of security functions behaviour

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

6.1.1.4.2 MANAGEMENT OF SECURITY ATTRIBUTES (FMT_MSA.1)

FMT_MSA.1/Administrator Management of security attributes

FMT_MSA.1.1 / Administrator	The TSF shall enforce the **SCD Import SFP and the Initialisation SFP** to restrict the ability to **modify [assignment: other operations]** the security attributes **SCD / SVD management** and **secure SCD import allowed** to **Administrator**.
Assignment	Other operations: ***none***

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1 / Signatory	The TSF shall enforce the **Signature-creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **Signatory**.

6.1.1.4.3 SECURE SECURITY ATTRIBUTES (FMT_MSA.2)

FMT_MSA.2 Secure security attributes

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

6.1.1.4.4 STATIC ATTRIBUTE INITIALISATION (FMT_MSA.3)

FMT_MSA.3 Static attribute initialisation

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 import of the SCD. The security attribute of the SCD “SCD operational” is set to “no” after generation of the SCD.
FMT_MSA.3.2	The TSF shall allow the **Administrator** to specify alternative initial values to override the default values when an object or information is created.

6.1.1.4.5 MANAGEMENT OF TSF DATA (FMT_MTD.1)

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1	The TSF shall restrict the ability to **modify [assignment: other operations]** the **RAD** to **Signatory**.
Assignment	Other operations: ***none***

6.1.1.4.6 SECURITY ROLES (FMT_SMR.1)

FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles **Administrator** and **Signatory**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.2 Protection of the TSF (FPT)

6.1.2.1 ABSTRACT MACHINE TESTING (FPT_AMT.1)

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1	The TSF shall run a suite of tests **[selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions]** to demonstrate the correct operation of the

	security assumptions provided by the abstract machine that underlies the TSF.
Selection	***during initial start-up***

6.1.2.2 TOE EMANATION (FPT_EMSEC.1)

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1	The TOE shall not emit **[assignment: types of emissions]** in excess of **[assignment: specified limits]** enabling access to **RAD** and **SCD**.
Assignment	Types of emissions: ***side channel*** Specified limits: ***state of the art***
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 **RAD** and **SCD**.
Assignment	Type of users: ***any user*** Type of connection: ***external interface***

Application note 9: The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

6.1.2.3 FAILURE WITH PRESERVATION OF SECURE STATE (FPT_FLS.1)

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[assignment: list of types of failures in the TSF]**.

Assignment	List of types of failures in the TSF: **(1) Exposure to out-of-range operating conditions where therefore a malfunction could occur,** **(2) Failure detected by TSF according to FPT_TST.1** ❑

6.1.2.4 PASSIVE DETECTION OF PHYSICAL ATTACK (FPT_PHP.1)

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.2.5 RESISTANCE TO PHYSICAL ATTACK (FPT_PHP.3)

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1	The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the SFR are always enforced.
Assignment	❑ Physical tampering scenarios: **physical manipulation and physical probing** List of TSF devices/elements: **TSF**

Application note 10: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here

- assuming that there might be an attack at any time and
- countermeasures are provided at any time.

6.1.2.6 TSF TESTING (FPT_TST.1)

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self tests **[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]** to demonstrate the correct operation of the TSF.
Selection	***during initial start-up***
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.2.7 TRUSTED PATH/CHANNELS (FTP)

6.1.2.7.1 INTER-TSF TRUSTED CHANNEL (FTP_ITC.1)

FTP_ITC.1/SCD Import Inter-TSF trusted channel

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 **[selection: the TSF, the remote trusted IT product]** to initiate communication via the trusted channel.
Selection	***the remote trusted IT product***
FTP_ITC.1.3 / SCD Import	The TSF or the remote trusted IT shall initiate communication via the trusted channel for **SCD import**.
Refinement	The mentioned remote trusted IT product is a SSCD of type 1.

FTP_ITC.1/ SVD Transfer Inter-TSF trusted channel

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 **[selection: the TSF, the remote trusted IT product]** to initiate communication via the trusted channel.
Selection	***the remote trusted IT product***
FTP_ITC.1.3 / SVD Transfer	The TSF or the remote trusted IT shall initiate communication via the trusted channel for **transfer of SVD**.
Refinement	The mentioned remote trusted IT product is a SSCD of type 1 for SVD import and the CGA for the SVD export.

Application note 11: FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

FTP_ITC.1/DTBS Import Inter-TSF trusted channel

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 **[selection: the TSF, the remote trusted IT product]** to initiate communication via the trusted channel.
Selection	***SCA***
FTP_ITC.1.3 / DTBS Import	The TSF or the remote trusted IT shall initiate communication via the trusted channel for **signing DTBS-representation**.
Refinement	The mentioned remote trusted IT product is the SCA.

6.1.2.7.2 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/TOE Trusted path

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 **[selection: the TSF, local users]** to initiate communication via the trusted path.
Selection	***local users***
FTP_TRP.1.3 / TOE	The TSF shall require the use of the trusted path for **[selection: initial user authentication, [assignment: other services for which trusted path is required]]**.
Selection	***initial user authentication***

6.1.3 Security Functional Requirements for the IT Environment

6.1.3.1 SIGNATURE KEY GENERATION (SSCD TYPE1)

6.1.3.1.1 CRYPTOGRAPHIC KEY GENERATION (FCS_CKM.1)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **List of approved algorithms and parameters**.
Assignment	Cryptographic key generation algorithm: **[R15]**, **[R16]**, [R19] Cryptographic key sizes: ***1024, 1280, 1536, 1792, 2048, 2560, 3072, 3584 and 4096 bits for RSA, and 192, 224, 256, 384 and 521 for Elliptic curves***

6.1.3.1.2 CRYPTOGRAPHIC KEY DESTRUCTION (FCS_CKM.4)

FCS_CKM.4/Type1 Cryptographic key destruction

FCS_CKM.4.1/Type1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Assignment	Cryptographic key generation algorithm: ***Key overwriting*** List of standards: ***None***

Application note 12: The cryptographic key SCD will be destroyed automatically after export.

6.1.3.1.3 CRYPTOGRAPHIC OPERATION (FCS_COP.1)

FCS_COP.1/CORRESP Cryptographic operation

FCS_COP.1.1 / CORRESP	The TSF shall perform **SCD / SVD correspondence verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **List of approved algorithms and parameters**.
Assignment	Cryptographic algorithm: ***one of the following:*** ❑ ***RSASSA PKCS1-v1_5 SHA-1*** *[R22]* ❑ ***RSASSA PKCS1-v1_5 SHA-256*** *[R22]* ❑ ***ISO15946 ECDSA*** Cryptographic key sizes: ***1024, 1280, 1536, 1792, 2048, 2560 or 3072 bits for RSA, and 192, 224, 256, 384 and 521 for Elliptic curves***

6.1.3.1.4 SUBSET ACCESS CONTROL (FDP_ACC.1)

FDP_ACC.1/SCD Export SFP Subset access control

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

6.1.3.1.5 BASIC DATA EXCHANGE CONFIDENTIALITY (FDP_UCT.1)

FDP_UCT.1/Sender Basic data exchange confidentiality

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

6.1.3.1.6 INTER-TSF TRUSTED CHANNEL (FTP_ITC.1)

FTP_ITC.1/SCD Export Inter-TSF trusted channel

FTP_ITC.1.1 / SCD Export	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 / SCD Export	The TSF shall permit **[selection: the TSF, the remote trusted IT product]** to initiate communication via the trusted channel.
Selection	***The TSF (the SSCD type 1)***
FTP_ITC.1.3 / SCD Export	The TSF or the SSCD type2 shall initiate communication via the trusted channel for **SCD Export**.
Refinement	The mentioned remote trusted IT product is a SSCD of type 2.

Application note 13: If the TOE exports the SVD to a SSCD Type 2 and the SSCD Type 2 holds the SVD then the trusted channel between the TOE and the SSCD type 2 will be required .

6.1.3.2 CERTIFICATION GENERATION APPLICATION (CGA)

6.1.3.2.1 CRYPTOGRAPHIC KEY DISTRIBUTION (FCS_CKM.2)

FCS_CKM.2/CGA Cryptographic key distribution

FCS_CKM.2.1 / CGA	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **qualified certificate** that meets the following: **List of approved algorithms and parameters**.

6.1.3.2.2 CRYPTOGRAPHIC KEY ACCESS (FCS_CKM.3)

FCS_CKM.3/CGA Cryptographic key access

FCS_CKM.3.1 / CGA	The TSF shall perform **import the SVD** in accordance with a specified cryptographic key access method **import through a secure channel** that meets the following: **[assignment: list of standards]**.
Assignment	List of standards: *[R15]***,** *[R16]*

6.1.3.2.3 DATA EXCHANGE INTEGRITY (FDP_UIT.1)

FDP_UIT.1/SVD Import Data exchange integrity

FDP_UIT.1.1 / SVD Import	The TSF shall enforce the **SVD Import SFP** to be able to **receive** user data in a manner protected from **modification and insertion** errors.
FDP_UIT.1.2 / SVD Import	The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

6.1.3.2.4 INTER-TSF TRUSTED CHANNEL (FTP_ITC.1)

FTP_ITC.1/ SVD Import Inter-TSF trusted channel

FTP_ITC.1.1 / SVD Import	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 / SVD Import	The TSF shall permit **[selection: the TSF, the remote trusted IT product]** to initiate communication via the trusted channel.
Selection	***The TSF (the CGA)***
FTP_ITC.1.3 / SVD Import	The TSF or the remote trusted IT shall initiate communication via the trusted channel for **import of SVD**.

6.1.3.3 SIGNATURE CREATION APPLICATION (SCA)

6.1.3.3.1 CRYPTOGRAPHIC OPERATION (FCS_COP.1)

FCS_COP.1/SCA Hash Cryptographic operation

FCS_COP.1.1 / SCA Hash	The TSF shall perform **hashing the DTBS** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **none** that meet the following: **List of approved algorithms and parameters**.
Assignment	Cryptographic algorithm: ***One of the following:*** ❑ ***SHA-1*** ❑ ***SHA-256***

6.1.3.3.2 DATA EXCHANGE INTEGRITY (FDP_UIT.1)

FDP_UIT.1/SCA DTBS Data exchange integrity

FDP_UIT.1.1 / SCA DTBS	The TSF shall enforce the **Signature-creation SFP** to be able to **transmit** user data in a manner protected from **modification, deletion and insertion** errors.
FDP_UIT.1.2 / SSC DTBS	The TSF shall be able to determine on receipt of user data, whether **modification, deletion and insertion** has occurred.

6.1.3.3.3 INTER-TSF TRUSTED CHANNEL (FTP_ITC.1)

FTP_ITC.1/ SCA DTBS Inter-TSF trusted channel

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

6.1.3.3.4 TRUSTED PATH (FTP_TRP.1)

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

FTP_TRP.1/SCA Trusted path

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

Selection	***initial user authentication***

6.1.4 Security Functional Requirements for the Non-IT Environment

R.Administrator_Guide Application of Administrator Guidance

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

R.Sigy_Guide Application of User Guidance

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

R.Sigy_Name Signatory’s name in the Qualified Certificate

The CSP shall verify the identity of the person to which a qualified certificate is issued according to the Directive **[R13]**, ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (d). The CSP shall verify that this person holds the SSCD which implements and stores the SCD corresponding to the SVD to be included in the qualified certificate.

6.2 SECURITY ASSURANCE REQUIREMENTS

The assurance level specified in the present security target and in its documentation is EAL 5 augmented by the following components defined in CC part 3 [R6]:

- ALC_DVS.2,
- AVA_VAN.5.

Table 6-1 list all the Assurance Requirements applicable.

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_IMP.1, ADV_INT.2, ADV_TDS.4
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1 ALC_TAT.2
ATE	ATE_COV.2, ATE_DPT.3, ATE_FUN.1, ATE_IND.2
AVA	AVA_ VAN.5

Table 6-1

As there is no specific operation or refinement on the security assurance requirements, they are not detailed in this security target.

6.2.1 Rationale for Assurance Level 5 Augmented

The assurance level for this ST is EAL5+ augmented. The TOE is semiformally designed and tested. EAL5+ allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. The TOE is intended to operate in open environments, where attackers can easily exploit vulnerabilities. According to the usage of the TOE, it represents a significant value to perform attacks. In some malicious usages, of the TOE the statistical or probabilistic mechanisms in the TOE, for instance, may be subjected to analysis and attack in the normal course of operation. This level seems to be the reasonable minimum level for card hosting sensitive operations.

Augmentation results from the selection of:

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

The TOE shall be protected in confidentiality and integrity during its development to meet the security objective OT.Lifecycle_Security. ALC_DVS.2 has no dependency.

AVA_VAN.5 Vulnerability Assessment - Vulnerability Analysis – Advanced Methodical Vulnerability Analysis

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VAN.5 has the following dependencies:

ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_IMP.1 Implementation representation of the TSF

ADV_TDS.3 Basic modular design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

All of these are met or exceeded in the EAL5+ assurance package.

6.2.2 Rationale for TOE assurance requirements conformance to PPs [R8] & [R9]

The set of assurance requirements has been chosen among component defined in CC v3.1 part 3, in a manner that ensures that all assurance requirements listed in PPs [R8] & [R9] and defined in CC v2.3 part 3 are fulfilled or exceeded.

[R8] & [R9] CC v2 assurance requirements	**TOE CC v3 assurance requirements**	**Rationale**
ADV_FSP.2	ADV_FSP.5	Both SARs require to provide functional specifications of the TOE. CC v3 ADV_FSP.5 additionally requires those

[R8] & [R9] CC v2 assurance requirements	TOE CC v3 assurance requirements	Rationale
		specifications to be written using a semi formal style.
	ADV_INT.2	This SAR is an augmentation to the PPs SARs.
ADV_HLD.2	ADV_TDS.4	The CC v3 ADV_TDS.4 requires the developer to provide a description of the sub-systems, which corresponds to the HLD description required by CC v2 ADV_HLD.2. CC v3 ADV_TDS.4 additionally requires this description to be written using a semi formal style.
ADV_IMP.1	ADV_IMP.1	Both SARs require to provide the implementation representation of the TSF to the evaluator for analysis.
ADV_LLD.1	ADV_TDS.4	The CC v3 ADV_TDS.4 requires the developer to provide a description of the modules, which corresponds to the LLD description required by CC v2 ADV_LLD.1. CC v3 ADV_TDS.4 additionally requires this description to be written using a semi formal style.
ADV_RCR.1	ADV_FSP.5 ADV_TDS.4	In CC v2, a specific SAR requires the developer to provide evidence at each description level of the TSF representation that the TSF is correctly and completely implemented, whereas in CC v3 the requirement for this rationale is done in each corresponding SAR.
ADV_SPM.1	ASE	The informal SPM is given by the collection of Security Objectives in the ST.
AGD_ADM.1	AGD_OPE.1	All available functions and interfaces with their use conditions, including the administration ones, are required by CC v3 AGD_OPE.1 to be described.
AGD_USR.1	AGD_OPE.1	All available functions and interfaces with their use conditions, including the user non-administration ones, are required by CC v3 AGD_OPE.1 to be described.
ALC_DVS.1	ALC_DVS.2	CC v3 ALC_DVS.1 is equivalent to CC v2 ALC_DVS.1. So CC v3 ALC_DVS.2 exceeds CC v2 ALC_DVS.1.
ALC_LCD.1	ALC_LCD.1	CC v3 ALC_ LCD.1 is equal to CC v2 ALC_ LCD.1.
ALC_TAT.1	ALC_TAT.2	CC v3 ALC_ TAT.2 is equivalent to CC v2 ALC_TAT.2, therefore the CC v2 ALC_TAT.1 is met.
ADO_DEL.2	ALC_DEL.1 AGD_PRE.1	CC v3 ALC_ DEL.1 is equivalent to CC v2 ADO_DEL.1. AGD_PRE.1 by requiring secure acceptance procedures allows to detect any modification during delivery if any.
ADO_IGS.1	AGD_PRE.1	CC v3 AGD_PRE.1 requires secure procedures for installation as well as CC v2 ADO_IGS.1 As the TOE is a smart card, the whole installation, generation and start-up of the TOE consist in powering the TOE and in verifying the value of the ATR.
ACM_AUT.1	ALC_CMC.4	CC v3 ALC_CMC requires at least as much as CC v2 ACM_AUT.1: use of a CM system, CM plan and documentation, automated measures for authorizing changes, automated means for TOE generation.
ACM_CAP.4	ALC_CMC.4 ALC_CMS.5	CC v3 ALC_CMC requires: unique TOE reference, use of a CM system, CM documentation, measures for authorizing changes, TOE generation, new item creation as well as CC v2 ACM_CAP.4. Other requirements of CC v2 ACM_CAP.4 are enforced by ALC_CMS.5: configuration list, unique identification for

[R8] & [R9] CC v2 assurance requirements	TOE CC v3 assurance requirements	Rationale
		each item.
ACM_SCP.2	ALC_CMS.5	CC v3 ALC_CMS.5 requires to provide a configuration list, including implementation representation, security flaws and evaluation evidence required by the SARs, as it is demanded by CC v2 ACM_SCP.2.
ATE_COV.2	ATE_COV.2	CC v3 ATE_COV.2 is equivalent to CC v2 ATE_COV.2 at the exception that the coverage is demonstrated using TSFI instead of TSF.
ATE_DPT.1	ATE_DPT.3	Both SARs define the depth at which the analysis of the testing coverage must be done. CC v3 ATE_DPT.3 requires the coverage to be demonstrated at the sub-system and module level, while CC v2 ATE_DPT.1 require the demonstration to be at the sub-system level (HLD) only.
ATE_FUN.1	ATE_FUN.1	CC v3 ATE_FUN.1 is equivalent to CC v2 ATE_FUN.1.
ATE_IND.2	ATE_IND.2	CC v3 ATE_IND.2 is equivalent to CC v2 ATE_IND.2.
AVA_MSU.3	AGD_OPE.1 AGD_PRE.1	The analysis of misuse of the guidances required by CC v2 AVA_MSU.3 is done through CC v3 AGD_OPE.1 and AGD_PRE.1.
AVA_SOF.1	AVA_ VAN.5	The analysis if the strength of the security functionality is done trough the TOE vulnerability analysis required by AVA_VAN.5.
AVA_VLA.4	AVA_ VAN.5	Both SARs require that the vulnerability testing shall be performed with a high level attack potential.

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 Security Requirement Coverage

The following tables in sub-section “Security Requirement Coverage” provide the mapping of the security requirements for the TOE and for the environment.

TOE SFR / 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	*O.Privacy*
FCS_CKM.1				X	X				X					
FCS_CKM.4		X		X									X	
FCS_COP.1/CORRESP					X									
FCS_COP.1/SIGNING												X		
FCS_COP.1/TDES														X
FCS_COP.1/MAC														X
FDP_ACC.1/SVD Transfer SFP						X								
FDP_ACC.1/Initialisation SFP			X	X										

TOE SFR / 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	*O.Privacy*
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/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			X
FIA_UID.1			X								X			X
FMT_MOF.1				X							X			
FMT_MSA.1/Administrator			X	X										
FMT_MSA.1/Signatory											X			
FMT_MSA.2											X		X	
FMT_MSA.3			X	X							X		X	
FMT_MTD.1											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/SCD Import													X	
FTP_ITC.1/SVD Transfer						X								
FTP_ITC.1/DTBS Import										X				
FTP_TRP.1/TOE											X			

Table 6.2: Functional Requirements to TOE Security Objective Mapping

Environment Security Requirements / Environment Security Objectives	OE.CGA_Qcert	OE.HI_VAD	OE.SCA_Data_Intend	OE.SVD_Auth_CGA	OE.SCD_SVD_Corresp	OE.SCD_Transfer	OE.SCD_Unique
FCS_CKM.1					X		X
FCS_CKM.4/Type1						X	

FCS_COP.1/CORRESP					X		
FDP_ACC.1/SCD Export SFP						X	
FDP_UCT.1/Sender						X	
FTP_ITC.1/SCD Export						X	
FCS_CKM.2/CGA	X						
FCS_CKM.3/CGA	X						
FCS_COP.1/SCA Hash			X				
FDP_UIT.1/SVD Import				X			
FTP_ITC.1/SVD Import				X			
FDP_UIT.1/SCA DTBS			X				
FTP_ITC.1/SCA DTBS			X				
FTP_TRP.1/SCA		X					
R.Sigy_Name	X						

Table 6.3: IT Environment Functional requirement to Environment Security Objective Mapping

Objectives	Requirements
OT.Lifecycle_Security	ALC_DVS.2, ALC_LCD.1, ALC_TAT.2, ALC_DEL.1, AGD_PRE.1
OT.SCD_Secrecy	ADV_IMP.1, AVA_VAN.5
OT.Sigy_SigF	AGD_PRE.1, AGD_OPE.1, AVA_VAN.5
OT.Sig_Secure	AVA_VAN.5
Security objectives	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_DPT.3, ATE_FUN.1, ATE_IND.2

Table 6.4: Assurance Requirement to Security Objective Mapping

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE SECURITY REQUIREMENTS SUFFICIENCY

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.

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

OT.SCD_Secrecy (Secrecy of signature-creation data) counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. When SCD/SVD pair is generated, OT.SCD_Secrecy is provided by the security functionalities specified by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by FMT_MOF.1, FMT_MSA.1/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 functionalities 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 functionalities specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functionalities or leak information of the SCD.

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

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation and AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functionalities are efficient.

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

OT.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_ITC.1/SCD Import and FDP_UCT.1/Receiver that ensure that a trusted channel is provided and that confidentiality is maintained. Security functionalities specified by FDP_ACC.1/SCD Import SFP, 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. Security functionality FCS_CKM.4 destroys the SCD before a SCD is re-imported into the TOE.

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity) covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of FDP_ITC.1/DTBS, FTP_ITC.1/DTBS Import, and by FDP_UIT.1/TOE DTBS. The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS. The access control requirements of FDP_ACC.1/Signature-creation SFP and FDP_ACF.1/Signature-creation SFP keeps 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 functionalities 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 and FMT_SMR.1 ensure that the signature process is restricted to the signatory.

The security functionalitiess specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, and 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 functionalities specified by FDP_SDI.2/Persistent and FPT_TRP.1/TOE ensure the integrity of stored data both during communication and while stored.

The security functionalities 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 AGC_OPE.1 and AGD_PRE.1 provide the misuse of the TOE implementation.

The assurance measures specified by AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functionalities 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 functionalities specified by FPT_TST.1 ensure that the security functionalities are performing correctly. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD) is provided by a trusted channel guaranteeing SVD origin and integrity by means of FTP_ITC.1/SVD Transfer and FDP_UIT.1/SVD Transfer. The cryptographic algorithms specified by FDP_ACC.1/SVD Transfer SFP, FDP_ACF.1/SVD Transfer SFP and FDP_ETC.1/SVD Transfer ensure that only authorised user can Import the SVD from a SSCD Type1 (if SCD is imported) and 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.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 define RAD as the corresponding user attribute. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3 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_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [R13], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

O.Privacy (Protection of TOE identification and of stored data) requires that the contactless interface does not allow an attacker to track the TOE or to get access to data stored on the TOE or exchanged with an authorized terminal. This is met by FIA_UID.1 and FIA_UAU.1 which requires that a terminal can only set up a trusted channel before it is identified and authenticated by the TOE, therefore an attacker will not be able to identify the TOE or interact with the TOE to get information. Setting up a trusted channel will also protect the exchanged data from disclosure. O.Privacy is also met by FCS.COP/TDES and FCS_COP.1/MAC, which allow to set up a secure messaging in integrity and confidentiality.

6.3.2.2 TOE ENVIRONMENT SECURITY REQUIREMENTS SUFFICIENCY

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

OE.SCD_Transfer (Secure transfer of SCD between SSCD) is provided by FDP_UCT.1/Sender, that ensure that a trusted channel is provided and that confidentiality is maintained. Security functionalities complying with FDP_ACC.1/Export SFP and FTP_ITC.1/ SCD Export ensure that only TOE may export the SCD. Security functionality specified by FCS_CKM.4/Type1 destroy the SCD, once exported from the TOE.

OE.SCD_Unique (Uniqueness of the signature-creation data) stores the requirement of practically unique SCD as laid down in the Directive [R13], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

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

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

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

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.Import which assures identification of the sender and by FDP_UIT.1/ SVD Import, which guarantees its integrity.

6.3.3 Dependency Rationale

6.3.3.1 FUNCTIONAL AND ASSURANCE REQUIREMENTS DEPENDENCIES

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 6.3.3.2 for justification).

Requirements		**Dependencies**
Functional Requirements		
FCS_CKM.1		FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4		FCS_CKM.1, FDP_ITC.1/SCD
FCS_COP.1/CORRESP		FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SIGNING		FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FDP_ITC.1/SCD
FCS_COP.1/TDES		FDP_ITC.1, FCS_CKM.1, FCS_CKM.4
FCS_COP.1.MAC		FDP_ITC.1, FCS_CKM.1, FCS_CKM.4
FDP_ACC.1/Initialisation SFP		FDP_ACF.1/Initialisation SFP
FDP_ACC.1/Personalisation SFP		FDP_ACF.1/Personalisation SFP
FDP_ACC.1/Signature-Creation SFP		FDP_ACF.1/ Signature-Creation SFP
FDP_ACC.1/SVD Transfer SFP		FDP_ACF.1/ SVD Transfer SFP
FDP_ACC.1/SCD Import SFP		FDP_ACF.1/ SCD Import SFP
FDP_ACF.1/Initialisation SFP		FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/Personalisation SFP		FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/ Signature-Creation SFP		FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP		FDP_ACC.1/ SVD Transfer SFP, FMT_MSA.3
FDP_ACF.1/ SCD Import SFP		FDP_ACC.1/ SCD Import SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP		FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/SCD		FDP_ACC.1/ SCD Import SFP, FMT_MSA.3
FDP_ITC.1/DTBS		FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
FDP_UCT.1/Receiver		FTP_ITC.1/ SCD Import SFP, FDP_ACC.1/ SCD Import SFP
FDP_UIT.1/SVD Transfer		FTP_ITC.1/ SVD Transfer, FDP_ACC.1/ SVD Transfer SFP
FDP_UIT.1/TOE DTBS		FDP_ACC.1/ Signature-Creation SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1		FIA_UAU.1
FIA_UAU.1		FIA_UID.1
FMT_MOF.1		*FMT_SMF.1*, FMT_SMR.1
FMT_MSA.1/Administrator		FDP_ACC.1/Initialisation SFP, FDP_ACC.1/ SCD Import SFP, *FMT_SMF.1*, FMT_SMR.1
FMT_MSA.1/Signatory		FDP_ACC.1/ Signature-Creation SFP, *FMT_SMF.1*, FMT_SMR.1
FMT_MSA.2		ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3		FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1		*FMT_SMF.1*, FMT_SMR.1
FMT_SMR.1		FIA_UID.1
FPT_FLS.1		ADV_SPM.1
FPT_PHP.1		FMT_MOF.1
FPT_TST.1		None
Assurance Requirements		
PPs SARs	**ST SARs**	
ACM_AUT.1	ALC_CMC.4	ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
ACM_CAP.4	ALC_CMC.4 ALC_CMS.5	ALC_CMS.1, ALC_DVS.2, ALC_LCD.1 /
ACM_SCP.2	ALC_CMS.5	/
ADO_DEL.2	ALC_DEL.1 AGD_PRE.1	/ /
ADO_IGS.1	AGD_PRE.1	/
	ADV_ARC.1	ADV_FSP.1, ADV_TDS.1
ADV_FSP.2	ADV_FSP.5	ADV_TDS.1, ADV_IMP.1

Requirements		Dependencies
ADV_HLD.2	ADV_TDS.4	ADV_FSP.5
ADV_IMP.1	ADV_IMP.1	ADV_TDS.3, ALC_TAT.1
	ADV_INT.2	ADV_IMP.1, ADV_TDS.3, ALC_TAT.1
ADV_LLD.1	ADV_TDS.4	ADV_FSP.5
ADV_RCR.1	ADV_FSP.5 ADV_TDS.4	ADV_TDS.1, ADV_IMP.1 ADV_FSP.5
ADV_SPM.1	ASE	ASE
AGD_ADM.1	AGD_OPE.1	ADV_FSP.1
AGD_USR.1	AGD_OPE.1	ADV_FSP.1
ALC_DVS.1	ALC_DVS.2	/
ALC_LCD.1	ALC_LCD.1	/
ALC_TAT.1	ALC_TAT.2	ADV_IMP.1
ATE_COV.2	ATE_COV.2	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	ATE_DPT.3	ADV_ARC.3, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_FUN.1	ATE_COV.1
ATE_IND.2	ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
AVA_MSU.3	AGD_OPE.1 AGD_PRE.1	ADV_FSP.1
AVA_SOF.1	AVA_VAN.5	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1
AVA_VLA.4	AVA_VAN.5	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1
Functional Requirements for Certification generation application (CGA)		
FCS_CKM.2/CGA		unsupported dependencies, see sub-section 6.3.3.2 for justification
FCS_CKM.3/CGA		unsupported dependencies, see sub-section 6.3.3.2 for justification
FDP_UIT.1/SVD Import		FTP_ITC.1/SVD Import, unsupported dependencies, see sub-section 6.3.3.2 for justification
FTP_ITC.1/SVD Import		None
Functional Requirements for Signature creation application (SCA)		
FCS_COP.1/SCA HASH		unsupported dependencies, see sub-section 6.3.3.2 for justification
FDP_UIT.1/SCA DTBS		FTP_ITC.1/ SCA DTBS, unsupported dependencies, see sub-section 6.3.3.2 for justification
FTP_ITC.1/SCA DTBS		None
FTP_TRP.1/SCA		None
Functional Requirement for SSCD Type1		
FCS_CKM.1		FCS_CKM.4/Type1, FCS_COP.1/CORRESP, unsupported dependencies, see sub-section 6.3.3.2 for justification
FCS_CKM.4/Type1		FCS_CKM.1, unsupported dependencies, see sub-section 6.3.3.2 for justification
FCS_COP.1/CORRESP		unsupported dependencies, see sub-section 6.3.3.2 for justification
FDP_ACC.1/SCD Export SFP		unsupported dependencies, see sub-section 6.3.3.2 for justification
FDP_UCT.1/Sender		FDP_ACC.1/SCD Export, FTP_ITC/SCD Export
FTP_ITC.1/SCD Export		None

Table 6.5: Functional and Assurance Requirements Dependencies

6.3.3.2 JUSTIFICATION OF UNSUPPORTED DEPENDENCIES

The security functional dependencies for the TOE environment SSCD Type1, CGA and SCA are not completely supported by security functional requirements in section 6.1.3.

FCS_CKM.1

The SSCD Type1 generates the SCD/SVD pair. The dependency for cryptographic secure key generation is supported by FCS_COP.1/CORRESP, proof of SCD/SVD correspondence, and the key destruction by FCS_CKM.4/Type1.

FCS_CKM.4/Type1

The SSCD Type1 destroys the SCD once it has been exported. The dependency for key generation is supported by FCS_CKM.1.

FCS_COP.1/ CORRESP

The SSCD Type1 does a cryptographic operation when creating the SCD/SVD pair, FCS_CKM.1 and when destroying it, FCS_CKM.4/Type1.

FDP/ACC.1/ SCD Export SFP

The SSCD Type1 will follow the SCD export SFP when exporting the SCD. The access control required by this SFP, FDP_ACF.1 Security attribute based access control, is outside the scope of this ST.

FCS_CKM.2/ CGA

The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA.

FCS_CKM.3/ CGA

The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA.

FDP_UIT.1/ SVD Import (CGA)

The access control (FDP_ACC.1) for the CGA is outside the scope of this Security Target.

FCS_COP.1/ SCA HASH

The hash algorithm implemented by FCS_COP.1/SCA HASH does not require any key or security management. Therefore FDP_ITC.1, FCS_CKM.1 and FCS_CKM.4 are not required for FCS_COP.1/SCA HASH in the SCA.

FDP_UIT.1/ SCA DTBS

Access control (FDP_ACC.1.1) for the SCA is outside of the scope of this Security Target.

FMT_MOF.1

The TOE manage management function only during personalization phases, therefore FMT_SMF.1 is not required.

FMT_MOF.1/administrator

The TOE manage management function only during personalization phases, therefore FMT_SMF.1 is not required.

FMT_MOF.1/Signatory

The TOE manage management function only during personalization phases, therefore FMT_SMF.1 is not required.

FMT_MTD.1

The TOE manage management function only during personalization phases, therefore FMT_SMF.1 is not required.

6.3.4 Security Requirements Grounding in Objectives

This chapter covers the grounding that has not been done in the precedent chapter.

Requirements		**Security Objectives**
PPs Security assurance requirements	**ST Security assurance requirements**	
ACM_AUT.1	ALC_CMC.4	EAL 5
ACM_CAP.4	ALC_CMC.4 ALC_CMS.5	EAL 5
ACM_SCP.2	ALC_CMS.5	EAL 5
ADO_DEL.2	ALC_DEL.1 AGD_PRE.1	EAL 5
ADO_IGS.1	AGD_PRE.1	EAL 5
ADV_FSP.2	ADV_FSP.5	EAL 5
	ADV_INT.2	EAL 5
ADV_HLD.2	ADV_TDS.4	EAL 5
ADV_IMP.1	ADV_IMP.1	EAL 5
ADV_LLD.1	ADV_TDS.4	EAL 5
ADV_RCR.1	ADV_FSP.5 ADV_TDS.4	EAL 5
ADV_SPM.1	ASE	EAL 5
AGD_ADM.1	AGD_OPE.1	EAL 5
AGD_USR.1	AGD_OPE.1	EAL 5
ALC_DVS.1	ALC_DVS.2	EAL 5, OT.Lifecycle_Security
ALC_LCD.1	ALC_LCD.1	EAL 5, OT.Lifecycle_Security
ALC_TAT.1	ALC_TAT.2	EAL 5, OT.Lifecycle_Security
ATE_COV.2	ATE_COV.2	EAL 5
ATE_DPT.1	ATE_DPT.3	EAL 5
ATE_FUN.1	ATE_FUN.1	EAL 5
ATE_IND.2	ATE_IND.2	EAL 5
AVA_MSU.3	AGD_OPE.1 AGD_PRE.1	OT.Sigy_SigF
AVA_SOF.1	AVA_VAN.5	OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	AVA_VAN.5	OT.SCD_Secrecy, OT.Sig_Secure,
Security requirements for the non IT environment		
R.Administrator_Guide		AGD_ADM.1
R.Sigy_Guide		AGD_USR.1
R.Sigy_Name		OE.CGA_QCert

Table 6.6: Assurance and Functional Requirement to Security Objective Mapping

7 TOE SUMMARY SPECIFICATION

7.1 SECURITY FUNCTIONALITY DESCRIPTION

7.1.1 Chip security functionalities

The following functionalities of the product are directly addressed by the chip. The complete list the chip security functionality can be check in the chip Security Target [R11].

TSF_INTEGRITY

This security functionality is responsible for:

- correcting single bit fails upon a read operation on each NVM byte,
- verifying valid CPU usage,
- checking integrity loss when accessing NVM, ROM or RAM,
- providing a sign engine to check code and/or data integrity loss,
- monitoring various manifestations of fault injection attempts,
- providing a security timeout feature (watchdog timer),
- providing the embedded software developer with the traceability information of the TOE.

TSF_PHYSICAL_TAMPERING

This security functionality ensures that:

- The TOE detects clock and voltage supply operating changes by the environment,
- The TOE detects attempts to violate its physical integrity, and glitch attacks,
- The TOE is always clocked with shape and timing within specified operating conditions.

TSF_SECURITY_ADMIN

This security functionality ensures the management of the following security violation attempts:

- Incorrect CPU usage,
- Integrity loss in NVM, ROM or RAM
- Code signature alarm,
- Fault injection attempt,
- access attempt to unavailable or reserved memory areas,
- MPU errors,
- Clock and voltage supply operating changes,
- TOE physical integrity abuse.

TSF_UNOBSERVABILITY

This security functionality prevents the disclosure of user data and of TSF data when it is transmitted between separate parts of the TOE (the different memories, the CPU and other functional units of the TOE such as a cryptographic co-processor are seen as separated parts of the TOE):

This functionality provides additional support mechanisms to the SICESW developer contributing to avoid information leakage.

TSF_SYM_CRYPTO

This security functionality provides DES and TDES data encryption / decryption capability, in order to compute Message Authentication code (MAC) or the encrypted data.

TSF_ASYM_CRYPTO

This security functionality provides:

- RSA verification (encryption) with an RSA modulo up to 4096 bits,
- RSA signature (decryption) using or not using the Chinese Remainder Theorem (CRT), with an RSA modulo up to 4096 bits,
- RSA private and public keys computation with an RSA modulo up to 4096 bits,
- Prime number generation up to 3200 bits, with Rabin-Miller primality tests.

This functionality implements also the following standard hash function:

- SHA-1 hash function chaining blocks of 512 bits to get a 160 bits result,
- SHA-224 hash function chaining blocks of 512 bits to get a 224-bit result,
- SHA-256 hash function chaining blocks of 512 bits to get a 256-bit result.

This security function provides also the following basic functions for Elliptic Curves Cryptography over prime fields:

- general point addition,
- point expansion and compression,
- public scalar multiplication,
- private scalar multiplication.

TSF_ALEAS

This security functionality provides a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. The RNG complies with the AIS31 Class P2 quality metric.

7.1.2 Low level security functionalities

TSF_PHYS

This security functionality provides protection mechanism of the TOE towards observation and physical tampering, such as random delay and desynchronisation capability. This security functionality may call TSF_UNOBSERVABILITY.

7.1.3 Operating system security functionalities

TSF_RNG

This security functionality manages random number generation in compliance with X9.31 **[R25]**. This function calls TSF_ALEAS to initialise the seed key.

TSF_ACCESS

This security functionality manages the access to objects (files, directories, data and secrets) stored in E²PROM.

Write and read access to RAM and ROM are forbidden from outside of the TOE.

Access to an object is granted if:

- Object type is managed by the TOE ;
- Object Integrity is verified ;
- Access conditions are fulfilled ;

Operations on objects are:

- File or directory creation with related security attributes. A file or directory is created under the ADF of the application with whom it is associated.
- File or directory deletion.
- Write operation.
- Read operation.
- Object life cycle management.
- SCD/SVD generation.
- SCD/SVD destruction.
- SCD Import.
- SVD Export.
- DTBS loading from an authorized SCA.
- DTBS signature with an operational SCD.

Access conditions are:

- The object must be under the ADF of the application, if an application is selected.
- There must be a consistency between the security state of the card and the access rights to the object. Access rights can be:
    - ALWAYS: Operation always authorized
    - NEVER: Operation never authorized
    - USERx: Operation authorized if USERx is authenticated

- SMI: Operation authorized if the command is protected in integrity by a secure messaging.
- SMI + SMC: Operation authorized if the command is protected in integrity and confidentiality by a secure messaging.

TSF_INIT

This security function is called after each reset of the card and performs the following operations:

- test of the TOE (call of the TSF_TEST security function) ;
- “Answer to Attrib” + “ATQB” emission ;
- Module initialization and application initialization.

TSF_MEMORY

This security functionality manages E²PROM and RAM erasure:

- RAM erasure is achieved by a software mechanism that writes random data in RAM;
- E²PROM erasure is achieved by a software mechanism that writes random data in E²PROM.

TSF_CHECK

This security functionality tests the integrity of the following items:

- File header: Checksum / E²PROM ;
- File body: Checksum / E²PROM ;
- OTP area: Checksum / E²PROM ;
- Secrets ;
- I/O buffers ;

When an error is detected, the TSF_AUDIT security functionality is called and TSF_AUDIT takes the appropriate actions.

TSF_TEST

This security functionality tests the following elements at start-up:

- E²PROM stored executable code
- ROM ;
- Random number generator ;
  - DES hardware ;
  - Crypto processor ;

Integrity of the executable code in EEPROM is also checked before its execution.

When an error is detected, the TSF_AUDIT security functionality is called and TSF_AUDIT takes the appropriate actions.

TSF_AUDIT

This security functionality is reacting when a fault or an anomaly is detected. In any case, the RAM is erased and a reset occurs. In some cases, the E²PROM may also be erased and the card will be terminated.

Exception	Type	E²PROM erasure and card termination
IT test	Anomaly	N.A.
Voltage sensor	Anomaly	N.A.
Frequency sensor	Anomaly	N.A.
Temperature sensor	Anomaly	N.A. (not available on ST23)
Erroneous OPCODE	Anomaly	No (reset only)
Error during RANDOM testing	Anomaly	No (reset only)
Error during Crypto-processor testing	Fault	Yes
DES Testing	Fault	Yes
CRC Testing	Fault	Yes
RAM writing/reading error test	Fault	Yes
Data integrity test	Fault	Yes
ROM code integrity test	Fault	Yes
OTP area integrity test	Fault	Yes
Code sequence testing during execution	Fault	Yes

7.1.4 Application manager security functions

TSF_GESTION

At start-up of the card, this security function calls TSF_INIT and then waits for a command sent by the terminal. This command is then executed or transmitted to another module or application.

This security function manages:

- Management of the secure state of the TOE.
- Application selection.
- Application separation.

Management of the secure state of the TOE:

The security function TSF_GESTION updates the security state of the TOE according to:

- Current authenticated user.
- Access conditions and validity of those access conditions.

Application selection and application separation:

The security function TSF_GESTION ensures that each received command is forwarded to the right application.

7.1.5 Application security functionalities

TSF_SECRET

This security function ensures secure management of secret such as cryptographic keys. All secrets are handled only by the Secret Management module (GS) and are identified through an identification number.

Secret management consists of the following functionalities:

- Session key generation (key derivation)
- Secret destruction
- Secret loading
- Secret transfer

Session key generation

Session keys are protected in integrity and confidentiality during generation. The Secret Management module (GS) enforces secure storage of the session keys during generation.

Secret destruction

The Secret Management module (GS) calls the security function TSF_MEMORY to erase keys.

Secret loading

Loading of a secret is always done by an authorized user through a secure command. This command is accepted only after authentication of the authorized user.

Secret transfer

The Secret Management module (GS) manage the secure transfer of every secret to the crypto-processor when used for cryptographic operation.

TSF_CRYPTO

This security functionality performs high level cryptographic operations:

- Encryption/decryption ;
- Integrity verification ;
- Authentication cryptogram creation/verification ;
- Key generation ;
- Electronic signature generation ;
- Asymmetric key pair consistency check
- Hash value calculation ;

This security functionality may call TSF_CL_CRYPTO and TSF_RNG.

Encryption/decryption

TSF_CRYPTO performs TDES in CBC mode in conformance with Triple Data Encryption Algorithm Modes of Operation ANSI X9.52 1998, American Bankers Association in order to achieve encryption and decryption in secure messaging.

Integrity verification

TSF_CRYPTO performs Retail MAC in conformance with ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2), in order to achieve message authentication code in secure messaging.

Authentication cryptogram creation/verification

TSF_CRYPTO performs the following authentication cryptogram calculation/verification:

- Mutual symmetric authentication based on TDES,
- External symmetric authentication based on TDES,
- External asymmetric authentication based on RSA.
- Mutual asymmetric authentication based on Diffie-Hellman and RSA.

Key generation

TSF_CRYPTO performs RSA key generation of size 1024, 1536, 2048, 2560, 3072, 3584 and 4096 bits in conformance with **[R15]** and **[R16]**. Key generation is performed based on random numbers generated by a deterministic RNG (call to TSF_RNG).

TSF_CRYPTO performs Elliptic curves generation of size 192, 224, 256, 384 and 521 bits.

Electronic signature generation

TSF_CRYPTO performs RSA with keys of size 1024, 1536, 2048, 2560, 3072 bits in conformance with RSA SSA pkcs1 v1.5 to achieve digital signature generation.

TSF_CRYPTO performs ECDSA with keys of size 192, 224, 256, 384 and 521 bits in conformance with ISO15946 ECDSA to achieve digital signature generation.

Asymmetric key pair consistency check

TSF_CRYPTO performs SCD/SVD consistency check before signature generation by signature generation followed by signature verification. If the signature verification does not match the signature generation, then the key pair is not consistent.

Hash value calculation

TSF_CRYPTO performs SHA-1 and SHA-256 in conformance with [FIPS180-2], in order to calculate a hash value.

TSF_AUTH

This security functionalities manages the authentication of the user, whether the signatory or the administrator.

The signatory gets authenticated by means of a secret password (PIN) or by a biometric data (MOC): TSF_AUTH verifies that the VAD (PIN or the fingerprint) presented by the user is identical to the RAD (PIN or the fingerprint)stored in the TOE .

The administrator gets authenticated by means of:

– a TDES key (external symmetric authentication based on TDES)

or

– a TDES key set (mutual symmetric authentication based on TDES)

or

– an RSA key (external asymmetric authentication based on RSA)

or

– an RSA key (mutual asymmetric authentication based on Diffie-Hellman and RSA)

or

– Password (PIN verification).

TSF_AUTH may call TSF_CRYPTO to perform authentication and may call TSF_RATIF for managing unsuccessful authentication attempts.

TSF_RATIF

A counter is associated to a secret and to the VAD (Key, PIN, MOC), which is used to count the number of successive unsuccessful authentication attempts. The counter is reinitialised when the authentication is successful. If the counter reaches its maximum value, then the related secret is blocked and cannot be used anymore.

7.2 SECURITY FUNCTIONALITY RATIONALE

Table 7-1 provides an overview on how the security functionalities of the TOE cover the SFRs for the TOE.

	TSF_INTEGRITY	TSF_PHYSICAL_TAMPERING	TSF_SECURITY_ADMIN	TSF_UNOBSERVABILITY	TSF_SYM_CRYPTO	TSF_ASYM_CRYPTO	TSF_ALEAS	TSF_PHYS	TSF_RNG	TSF_ACCESS	TSF_INIT	TSF_MEMORY	TSF_CHECK	TSF_TEST	TSF_AUDIT	TSF_GESTION	TSF_SECRET	TSF_CRYPTO	TSF_AUTH	TSF_RATIF
FCS_CKM.1						**X**	**X**		**X**								**X**	**X**		
FCS_CKM.4												**X**					**X**			
FCS_COP.1 / CORRESP						**X**												**X**		
FCS_COP.1 / SIGNING						**X**												**X**		
FCS_COP.1 / TDES					**X**													**X**		

	TSF_INTEGRITY	TSF_PHYSICAL_TAMPERING	TSF_SECURITY_ADMIN	TSF_UNOBSERVABILITY	TSF_SYM_CRYPTO	TSF_ASYM_CRYPTO	TSF_ALEAS	TSF_PHYS	TSF_RNG	TSF_ACCESS	TSF_INIT	TSF_MEMORY	TSF_CHECK	TSF_TEST	TSF_AUDIT	TSF_GESTION	TSF_SECRET	TSF_CRYPTO	TSF_AUTH	TSF_RATIF
FCS_COP.1 / MAC					X													X		
FDP_ACC.1 / SVD Transfer SFP										X						X				
FDP_ACC.1 / SCD Import SFP										X						X				
FDP_ACC.1 / Personalisation SFP										X						X				
FDP_ACC.1 / Signature-creation SFP										X						X				
FDP_ACC.1 / Initialisation SFP										X						X				
FDP_ACF.1 / SVD Transfer SFP										X						X				
FDP_ACF.1 / SCD Import SFP										X						X				
FDP_ACF.1 / Personalisation SFP										X						X				
FDP_ACF.1 / Signature-creation SFP										X						X				
FDP_ACF.1 / Initialisation SFP										X						X				
FDP_ETC.1 / SVD Transfer										X										
FDP_ITC.1 / SCD										X										
FDP_ITC.1 / DTBS										X										
FDP_RIP.1												X								
FDP_SDI.2 / Persistent	X												X		X					
FDP_SDI.2 / DTBS	X												X		X					
FDP_UCT.1 / Receiver					X					X						X		X		
FDP_UIT.1 / SVD Transfer					X					X						X		X		
FDP_UIT.1 / TOE DTBS					X					X						X		X		
FIA_AFL.1																				X
FIA_ATD.1										X									X	
FIA_UAU.1										X	X					X			X	
FIA_UID.1										X	X					X				
FMT_MOF.1										X										
FMT_MSA.1 / Administrator										X										
FMT_MSA.1 / Signatory										X										
FMT_MSA.2										X										
FMT_MSA.3										X										
FMT_MTD.1										X										
FMT_SMR.1										X									X	
FPT_EMSEC.1				X				X									X	X		
FPT_FLS.1		X	X												X					
FPT_PHP.1		X	X												X					
FPT_PHP.3		X	X												X					
FPT_TST.1	X												X	X						
FTP_ITC.1 / SCD Import					X					X								X		
FTP_ITC.1 / SVD Transfer					X					X								X		

	TSF_INTEGRITY	TSF_PHYSICAL_TAMPERING	TSF_SECURITY_ADMIN	TSF_UNOBSERVABILITY	TSF_SYM_CRYPTO	TSF_ASYM_CRYPTO	TSF_ALEAS	TSF_PHYS	TSF_RNG	TSF_ACCESS	TSF_INIT	TSF_MEMORY	TSF_CHECK	TSF_TEST	TSF_AUDIT	TSF_GESTION	TSF_SECRET	TSF_CRYPTO	TSF_AUTH	TSF_RATIF
FTP_ITC.1 / DTBS Import					**X**					**X**								**X**		
FTP_TRP.1 / TOE					**X**					**X**								**X**		

Table 7-1: Coverage of SFR for the TOE by the TOE security functionality

FCS_CKM.1 is met by TSF_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs of size 1024, 1280, 1536, 1792 and 2048 bits in conformance with **[R15]** and **[R16]** and the ECDSA cryptographic key pairs of size 192, 224, 256, 384 and 521 bits. TSF_RNG and TSF_CL_CRYPTO, by providing random numbers, also support this requirement.

FCS_CKM.1 is also met by TSF_ASYM_CRYPTO, which provides RSA and ECDSA calculation.

FCS_CKM.1 is also met by TSF_SECRET, which ensures the protection of the keys during generation.

FCS_CKM.1 is also met by TSF_RNG and TSF_ALEAS, which provide generation of random number.

FCS_CKM.4 is met by TSF_SECRET and TSF_MEMORY, as TSF_SECRET manages the secure destruction of secret by calling TSF_MEMORY, and TSF_MEMORY manages erasure of data stored in E²PROM and RAM, and in particular of the SCD.

FCS_COP.1/CORRESP is met by TSF_CRYPTO that provides RSA and ECDSA key pair consistency check. TSF_ASYM_CRYPTO, by providing functionalities for RSA and basic functions for Elliptic Curves Cryptography, also supports this requirement.

FCS_COP.1/SIGNING is met by TSF_CRYPTO that provides electronic signature generation compliant with RSA SSA pkcs1 v1.5. and with ISO15946 ECDSA. TSF_ASYM_CRYPTO, by providing RSA and ECDSA functionalities, also supports this requirement.

FCS_COP.1/TDES is met by TSF_CRYPTO that provides TDES in CBC mode for encryption and decryption compliant with ANSI X9.52. TSF_SYM_CRYPTO, by providing TDES functionalities, also supports this requirement.

FCS_COP.1/MAC is met by TSF_CRYPTO that provides Retail MAC for integrity compliant with ISO 9797 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). TSF_SYM_CRYPTO, by providing TDES functionalities, also supports this requirement.

FDP_ACC.1/SVD Transfer SFP and **FDP_ACF.1/SVD Transfer SFP** are met by TSF_ACCESS that ensures that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by TSF_GESTION, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/SCD Import SFP and **FDP_ACF.1/SCD Import SFP** are met by TSF_ACCESS that ensures that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as authorized administrator or signatory can perform SCD import, and by TSF_GESTION, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/Personalisation SFP and **FDP_ACF.1/Personalisation SFP** are met by TSF_ACCESS that ensures that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only a user authenticated as administrator can perform RAD creation, and by TSF_GESTION, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/Signature-creation SFP and **FDP_ACF.1/ Signature-creation SFP** are met by TSF_ACCESS that ensures that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA or ECDSA key pair whose consistency has been verified, and by TSF_GESTION, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/Initialisation SFP and **FDP_ACF.1/Initialisation SFP** are met by TSF_ACCESS that ensures that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by TSF_GESTION, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ETC.1/SVD Transfer is met by TSF_ACCESS that ensures that only an authorized user under specific conditions can perform a dedicated operation, such as SVD export.

FDP_ITC.1/SCD is met by TSF_ACCESS that ensures that all the required conditions are met before allowing an operation such as SCD import.

FDP_ITC.1/DTBS is met by TSF_ACCESS that ensures that all the required conditions are met before allowing an operation such as signature generation and DTBS loading.

FDP_RIP.1 is met by TSF_MEMORY that ensure secure erasure of data in E²PROM and in RAM, and in particular of SCD, VAD and RAD.

FDP_SDI.2/Persistent and **FDP_SDI.2/DTBS** are met by TSF_INTEGRITY and by TSF_CHECK, that ensure the integrity of data stored in the TOE, and by TSF_AUDIT that ensures that the proper reaction is

taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_UCT.1/Receiver is met by TSF_ACCESS and TSF_GESTION that ensure that all the conditions are met before allowing an operation such as SCD import, and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide the cryptographic means to protect the SCD from disclosure during its import.

FDP_UIT.1/SVD Transfer is met by TSF_ACCESS and TSF_GESTION that ensure that all the conditions are met before allowing an operation such as SVD transfer and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide the cryptographic means to protect the SVD from unauthorized modification and insertion during its transfer.

FDP_UIT.1/TOE DTBS is met by TSF_ACCESS and TSF_GESTION that ensure that all the conditions are met before allowing an operation such as DTBS loading and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide the cryptographic means to protect the DTBS from unauthorized modification and insertion during their loading.

FIA_AFL.1 is met by TSF_RATIF that ensures that the RAD is blocked after a defined number of failed successive signatory authentication attempts.

FIA_ATD.1 is met by TSF_AUTH that linked the RAD to the signatory and by TSF_ACCESS that grants to the RAD owner specific access rights.

FIA_UAU.1 is met by TSF_INIT and TSF_GESTION, which manage the initialization of the communication with the card, by TSF_AUTH that ensures user authentication and by TSF_ACCESS that ensures that no operation is performed if the access conditions, such as user authentication, are not met.

FIA_UID.1 is met by TSF_INIT and TSF_GESTION, which manage the initialization of the communication with the card and by TSF_ACCESS that ensures that no operation is performed if the access conditions, such as user identification, are not met.

FMT_MOF.1 is met by TSF_ACCESS that ensures that only authenticated signatory can perform DTBS signature.

FMT_MSA.1/Administrator and **FMT_MSA.1/Signatory** are met by TSF_ACCESS that manages the access right policy of the TOE.

FMT_MSA.2 is met by TSF_ACCESS that manages the access right policy of the TOE and in particular manages the security attributes.

FMT_MSA.3 is met by TSF_ACCESS that manages the access right policy of the TOE and in particular manages the security attributes, their initialisation and their access rights.

FMT_MTD.1 is met by TSF_ACCESS that ensures that only authenticated signatory can modify the RAD.

FMT_SMR.1 is met by TSF_AUTH that provide user authentication as administrator or as signatory and by TSF_ACCESS that grants to the administrator and to the signatory specific access rights, thus defining roles for the TOE.

FPT_EMSEC is met by TSF_UNOBSERVABILITY and TSF_PHYS that ensure that no emanation can be used to retrieve information during TOE operations. FPT_EMSEC.1 is also met by TSF_CRYPTO and TSF_SECRET which ensure secure execution of cryptographic operations on keys.

FPT_FLS.1 is met by TSF_PHYSICAL_TAMPERING, TSF_SECURITY_ADMIN and TSF_AUDIT that ensures that failures in the TSF are detected and that the proper actions (reset, card termination…) are taken in order to preserve a secure sate of the TOE.

FPT_PHP.1 is met by TSF_PHYSICAL_TAMPERING, TSF_SECURITY_ADMIN and TSF_AUDIT that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination…) are taken, so that is can be determined if a physical tampering has occurred.

FPT_PHP.3 is met by TSF_PHYSICAL_TAMPERING, TSF_SECURITY_ADMIN and TSF_AUDIT that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination…) in order to protect the TOE.

FPT_TST.1 is met by TSF_TEST that performs a set of self-tests at start-up, thus checking the correct operation of the TSF, and that verifies the integrity of the stored executable code before or during its execution and by TSF_INTEGRITY and TSF_CHECK that provide means to verify the integrity of the data stored on the TOE.

FTP_ITC.1/SCD Import is met by TSF_ACCESS that enforces the access right policy for SCD Import and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SSCD type 1 to protect the exchanged data from modification and disclosure.

FTP_ITC.1/SVD Transfer is met by TSF_ACCESS that enforces the access right policy for SVD Transfer and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SSCD type 1 or a CGA to protect the exchanged data from modification and disclosure.

FTP_ITC.1/DTBS Import is met by TSF_ACCESS that enforces the access right policy for DTBS Import and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SCA to protect the exchanged data from modification and disclosure.

FTP_TRP.1/TOE is met by TSF_ACCESS that enforces the access right policy for initial user authentication and by TSF_CRYPTO and TSF_SYM_CRYPTO that provide cryptographic means for user authentication and to set up a trusted path to protect the exchanged data from modification and disclosure.

8 DEFINITIONS, GLOSSARY AND ACRONYMS

8.1 GLOSSARY

Administrator means a user that performs TOE initialisation, TOE personalisation, or other TOE administrative functions.

Advanced electronic signature (defined in the Directive [R13], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

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

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN). The SSCD Protection Profile (PP) [R8] & [R9] represent Annex A to the CWA that has been developed by the European Electronic Signature Standardisation Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area F on secure signature-creation devices (SSCD).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [R13], article 2.9)

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

(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

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 [R13], article 2.11)

Data to be signed (DTBS) means the complete electronic data to be signed (including both user message and signature attributes).

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is

(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) 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
(c) or the hash-value in case
(d) is calculated by the TOE.

Directive The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [R13] is also referred to as the 'Directive' in the remainder of the PP.

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [R13] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [R13]. (defined in the Directive [R13], article 2.10)

Qualified electronic signature means an advanced signature which is based on a qualified certificate and which is created by a SSCD according to the Directive [R13], article 5, paragraph 1.

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

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 [R13]. (SSCD is defined in the Directive [R13], article 2.5 and 2.6).

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 [R13], article 2.3).

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

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.

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 [R13], article 2.4).

Signature-creation system (SCS) means the overall system that creates an electronic signature. The signature-creation system consists of the SCA and the SSCD.

Signature-verification data (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [R13], article 2.7)

Signed data object (SDO) means the electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

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

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

8.2 ACRONYMS

CC	Common Criteria
CGA	Certification Generation Application
CM	Configuration Management
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
IAS	Identité Authentification Signature
ICAO	International Civil Aviation Organization
IT	Information Technology
JCRE	Java Card Runtime Environment
JVM	Java Virtual Machine
OS	Operating System
PP	Protection Profile
RAD	Reference Authentication Data
RNG	Random Number Generator
SAR	Security Assurance Requirement
SCA	Signature-Creation Application
SCD	Signature-Creation Data
SCS	Signature-Creation System

SDO	Signed Data Object
SFP	Security Function Policy
SFR	Security Functional Requirement
SSCD	Secure Signature-Creation Device
ST	Security Target
SVD	Signature-Verification Data
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VAD	Verification Authentication Data
VGP	Visa Global Platform

9 REFERENCE AND APPLICABLE DOCUMENTS

9.1 REFERENCE DOCUMENTS

Designation	Reference	Title	Revision	Date
Common Criteria v2.3				
[R1]	CCMB-2005-08-001	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	Version 2.3	August 2005
[R2]	CCMB-2005-08-002	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	Version 2.3	August 2005
[R3]	CCMB-2005-08-003	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	Version 2.3	August 2005
Common Criteria v3.1				
[R4]	CCMB-2009-07-001	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	Version 3.1, Revision 3	July 2009
[R5]	CCMB-2009-07-002	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	Version 3.1, Revision 3	July 2009
[R6]	CCMB-2009-07-003	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	Version 3.1, Revision 3	July 2009
[R7]	CCMB-2007-09-004	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology	Version 3.1, Revision 2	September 2007
Protection Profiles and Security Target				
[R8]	PP0005	Protection Profile - Secure Signature-Creation Device Type 2	Version 1.04	25 July 2001
[R9]	PP0006	Protection Profile - Secure Signature-Creation Device Type 3	version 1.05	25 July 2001
[R10]	BSI-PP-0002-2001	Protection Profile, Security IC Platform Protection Profile. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik).	Version 1.0	July 2001
[R11]	SMD_SB23YR80_ST_09_001	SB23YR80B Security Target - Public Version	Rev 01.00	March 2009
[R11]	ANSSI-2010/02	SB23YR80 Version B with NesLib Version 3 – Chip Certificate	Version 1.0	January 2010

Designation	Reference	Title	Revision	Date
Technical or legal specifications				
[R13]	199/93/EC	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures Passports with Biometric Identification Capability.		13 December 1999
[R14]		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.		
[R15]	CWA 14890-1	CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements – (AREA-K-1)		April 2004
[R16]	CWA 14890-2	CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional Services – (AREA-K-2)		May 2004
[R17]		Plate-forme commune pour l'eAdministration – Spécification technique	Version 1.01	
[R18]	ICAO Doc 9303	part 1 volume 1, Sixth edition, 2006, Passports with Machine Readable Data Stored in Optical Character Recognition Format; part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability.	Sixth edition	2006
[R19]		The Elliptic Curve Digitale Signature Algorithm (ECDSA)		
CC supporting document				
[R20]	CCDB-2008-04-001	Supporting Document - Mandatory Technical Document - Application of Attack Potential to Smartcards	V2.5, R1	April 2008
[R21]	CCDB-2007-09-001	Supporting Document - Mandatory Technical Document - Composite product evaluation for Smartcards and similar devices	V1.0, R1	September 2007

9.2 APPLICABLE DOCUMENTS

Designation	Reference	Title	Revision	Date
Cryptography				
[R22]	RSASSA-PKCS1-v1_5	RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard	Version 2.1	June 14, 2002
[R23]	ISO/IEC 15946	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.		2002
[R24]	FIPS PUB 46-3	Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standards (DES), U.S. Department Of Commerce / National Institute of Standards and Technology.		Reaffirmed 1999 October 25
[R25]	ANSI X9.31	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 - Appendix A.2.4		1998
[R26]		Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology		2002 August 1
OTHER				
[R27]		VISA global platform requirements configuration 3 – compact	v2.1.1	May 2003
[R28]		Java Card 2.2.2 - Application Programming Interfaces, Sun Microsystems	V2.2.2	March 2006
[R29]		Java Card 2.2.2 - JCRE, Sun Microsystems	V2.2.2	March 2006
[R30]		Java Card 2.2.2 - Virtual Machine Specifications, Sun Microsystems	V2.2.2	March 2006
[R31]		Plate-forme commune pour l'eAdministration – Spécification technique	Version 1.01	
[R32]		EMV CPS	1.0 Final	16 June 2003
[R33]	ANSI X9.31	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) - Appendix A.2.4		1998