Austria Card GmbH
Lamezanstrasse 4-8
1232 Vienna
Austria

Security Target
T-Systems-DSZ-CC-04164

Version 1.7

July 9th, 2008

Evaluation of the ACOS EMV-A04V1, Configuration A

Developed and provided by

Austria Card

According to the

Common Criteria for Information Technology

Evaluation (CC) at Level EAL4+

by

Austria Card Gesellschaft m.b.H. Lamezanstr. 4-8, A-1232 Wien

Revision history

Version	Date	Changes	Remarks
Version 0.1	Nov. 25th, 2005	based on the SSCD PP and the ACOS-A03V0 ST	
Version 0.2	Jan. 25th, 2006	adjusted key lengths, algorithms, updated references	
Version 0.3	Feb. 10th, 2006	removed restriction that new signature keys cannot be generated after the old keys have been deleted	
Version 0.4	Feb. 14th, 2006	Split into Configuration A and Configuration B	
Version 0.5	Feb. 22nd, 2006	Minor editorial changes	
Version 1.0	Mar. 3rd, 2006	Minor editorial changes, first release version	
Version 1.1	April 10th, 2006	Changes as requested by evaluator; renamed ACOS A04	
Version 1.2	May 11th, 2006	Changed TOE description as requested by evaluator; disallowed re-generation of SCD	
Version 1.3	January 25th, 2008	Changed names of card life-cycles; updated references to signature law and chip type; table 6.1 updated	
Version 1.4	April 3rd, 2008	Chip type and identification corrected; references updated; description of TEST_ROM and TEST_RAM changed.	
Version 1.5	June 13th, 2008	Table 2.1 corrected	
Version 1.6	July 4th, 2008	Version of Administrator Guidance corrected	
Version 1.7	July 9th, 2008	Version of Command Specification corrected	

Last version: Version 1.7 (July 9th, 2008)

Table of content

Copyright

Invariant of the document

Invariant	Value (edit here)	Test output
name and file length	automatically set	security_target_acosA04V1_v1.7_confA.doc (1234944 Byte)
last version	Version 1.7	Version 1.7
date of this version	July 9th, 2008	July 9th, 2008
confidentiality	Company-confidential	Company-confidential
Name of the TOE (short)	ACOS EMV-A04V1 Conf. A	ACOS EMV-A04V1 Conf. A
Name of the TOE (long)	ACOS EMV-A04V1 Configuration A	ACOS EMV-A04V1 Configuration A
Sponsor (long)	Austria Card Gesellschaft m.b.H. Lamezanstr. 4-8, A-1232 Wien	Austria Card Gesellschaft m.b.H. Lamezanstr. 4-8, A-1232 Wien
Sponsor (short)	Austria Card	Austria Card
Certification ID Configuration A	T-Systems-DSZ-CC-04164	T-Systems-DSZ-CC-04164
certific. body (long)	T-Systems GEI GmbH	T-Systems GEI GmbH
certific. body (short)	T-Systems	T-Systems
List of authors	Thomas Aichinger, Christian Schwaiger, Rania Wazir	Thomas Aichinger, Christian Schwaiger, Rania Wazir

Document Organisation

The document is organised according to [1], Annex C.

Section 1 provides the introductory material for the Security Target (ST) which can be used as a secure signature-creation device (SSCD). The ST is based on the SSCD Type 3, Version 1.05 [17] Protection Profile (PP).

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [2] and Part 3 [3], that must be satisfied by the TOE.

Section 6 contains the TOE Summary Specification and defines 10 security functions SF1 to SF10 define the instantiation of the security requirements for the TOE. This specification provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

Section 7 contains PP conformance claims for the TOE.

Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 8 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A glossary is provided in section 9 to define frequently used terms and expressions.

An abbreviation list is provided in section 10 for frequently used abbreviations.

Section 11 provides references to identify background material used throughout the ST.

1 ST Introduction

1.1 ST identification

Title:	Security Target ACOS EMV-A04V1 Configuration A
Authors:	Austria Card Gesellschaft m.b.H. Lamezanstr. 4-8, A-1232 Wien
General Status:	draft
Vetting Status:	not evaluated
CC Version:	2.3
Version Number:	Version 1.7, July 9th, 2008
Registration:	T-Systems-DSZ-CC-04164
TOE name & version:	ACOS EMV-A04V1 Configuration A
Keywords:	secure signature-creation device, electronic signature, ACOS EMV-A04V1 Configuration A

1.2 ST overview

The TOE is Austria Card's ACOS EMV-A04V1 Configuration A. The TOE is contained in a smart card consisting of:

(i) The TOE

(ii) Data of other applications.

The TOE itself consists of:

(i) the hardware, which is the which is the NXP SmartMx P5CC037V0A

(ii) all executable code residing on the card

(iii) all data required for the digital signature application.

The TOE will be used as a secure signature-creation device (SSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures according to Directive 1999/93/ec on a community framework for electronic signatures (also referred to as the directive) [5], the Austrian Signaturgesetz [6] – [10] and the German Signaturgesetz [14] – [15].

Besides the secure signature creation function the smart card offers several different applications, for example an international EMV Application with DDA according to EMV2000.

The TOE has the possibility to generate secure signature RSA or ECC Key pairs up to a key length of 2048 bits and 256 bits respectively within the TOE using the random number generator of the ICC. Digital signature creation is done according to the standards

(1) RSA digital signature creation: PKCS#1, v2.1 [21]

(2) ECC digital signature creation: ECDSA [22]

(3) SHA-1, SHA-224, SHA-256: FIPS 180-2 [20]

The communication between the TOE and its environment can be established using secure messaging. Therefore, the TOE implements several key agreement protocols. The secure messaging mechanism used is based on 3DES encryption and decryption as defined in NIST Special Publication 800-67 [24].

The TOE mandates the use of secure messaging between the TOE and the IT-environment, i.e. it mandates the use of secure messaging between the TOE and the CGA (certification generation application) entity of the IT-environment and mandates secure messaging between the TOE and the SCA (signature creation application) entity of the IT-environment.

To protect access to sensitive data elements within the TOE, the TOE implements a state machine which allows the access of particular data elements only after authentication with the proper key or PIN/PUK.

1.3 CC conformance

The ST is CC Part 2 [2] extended and CC Part 3 [3] augmented.

The assurance level for this ST is EAL4 augmented. The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High).

The TOE is conformant to SSCD Type 3, Version 1.05 [17].

2 TOE description

The TOE is Austria Card's ACOS EMV-A04V1 Conf. A. The TOE will be used as secure signature-creation device (SSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures according to [5], [6] and [14].

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 is provided by the signature-creation application SCA as appropriate TOE environment,
  (b) using appropriate hash functions that are, according to [18], [19], agreed upon as suitable for qualified electronic signatures,
  (c) after appropriate authentication of the signatory by the TOE,
  (d) using appropriate cryptographic signature functions that employ appropriate cryptographic parameters in compliance with [18], [19].

Figure 1 shows the TOE scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the secure SCD/SVD generation, secure SCD storage and use, and signature-creation functionality. The CGA and the SCA (and possibly other applications) are part of the immediate environment of the TOE. The CGA shall communicate with the TOE over a trusted channel to receive the SVD generated by the TOE and to include the SVD in the certificate generated by the CGA. The human interface device provided by the SCA is used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD. The SCA establishes a trusted path to the TOE to protect the confidentiality and integrity of the VAD. The SCA establishes a trusted channel to the TOE to protect the integrity of the DTBS. The TOE requires the SCA to use a trusted path for sending the VAD and to use a trusted channel for sending the DTBS.

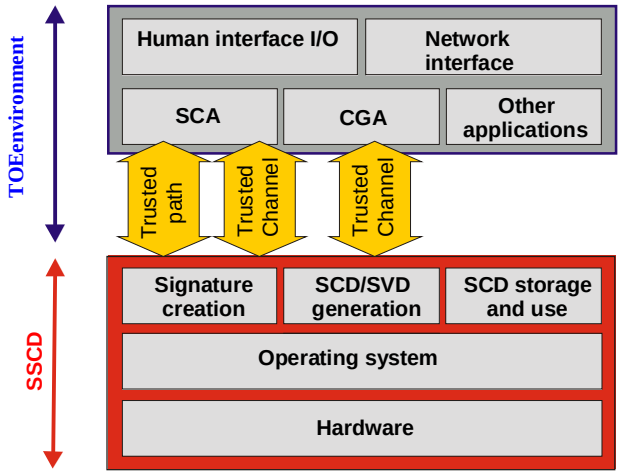

Figure 1: Scope of the SSCD, structural view

The TOE life cycle is shown in Figure 2. Basically, it consists of the development phase and the operational phase. The operational phase starts after initialisation with personalisation for the signatory's use by

(1) generating a SCD/SVD pair
(2) creation of the signatory's verification authentication data (SVAD).

The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., secure SCD storage and SCD use). The TOE implements all IT security functionality, which are necessary to ensure the secrecy of the SCD. 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 SVD corresponding

to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). To prevent the unauthorised usage of the SCD, the TOE provides user authentication and access control. The TOE will destroy the SCD, if it is no longer used for signature generation. The life cycle of the device as SSCD ends with the destruction of all SCD within the device.

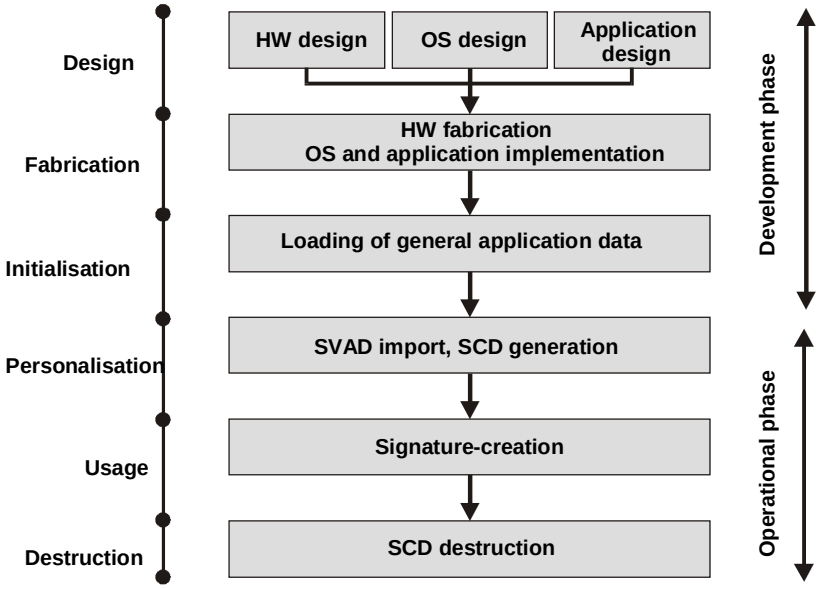

Figure 2 SSCD life cycle

The TOE as multi-application smart card implements additional functions and security features, but these are not subject of this ST.

The TOE provides a single physical interface over a serial connection according to [26] which is used to transmit command APDUs to the TOE and receive the corresponding response APDUs from the TOE as specified in [28] and in [29].

The following Table 2.1 lists the TOE's components.

Table 2.1: TOE deliverables

No	Type	Name	Form of delivery
1	HW/SW	NXP SmartMx P5CC037V0A with Austria Card ROM Mask AC_A04_V1R1.hex of 18.12.2007	Smart card with ROM code
2	SW	Digital Signature Application according to [30]	EEPROM
3	Doc	Administrator Guidance (AGD_ADM), Version 1.2, Austria Card, 2008 [31]	Copy or pdf
4	Doc	User Guidance (AGD_USR), Version 1.0, Austria Card, 2008 [32]	Copy or pdf
5	Doc	Specification of the generic Secure Signature Application for ACOS EMV-A04, Version 1.1, Austria Card, 2008 [30]	Copy or pdf
6	Doc	Delivery and Operation Documentation – Delivery, Installation and Generation, Version 1.2, Austria Card, 2008 [33]	Copy or pdf
7	Doc	ACOS EMV-A04 Commands, Version 2.1, Austria Card, 2008, [34]	Copy or pdf
8	Doc	ACOS EMV-A04 Init-Pers-Concept, Version 1.3, Austria Card, 2008 [35]	Copy or pdf

3 TOE security environment

Assets:

1. **SCD**: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
2. **SVD**: public key linked to the SCD and used to perform an electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. **DTBS** and **DTBS-representation**: set of data, or its representation which is intended to be signed. Their integrity must be maintained.
4. **VAD**: PIN code or biometric data entered by the End User to perform a signature operation. The confidentiality and authenticity of the VAD as required by the authentication method employed must be maintained.
5. **RAD**: Reference PIN code or biometric authentication reference used to identify and authenticate the End User. The integrity and confidentiality of RAD must be maintained.
6. **Signature-creation function** of the SSCD using the SCD: The quality of the function must be maintained so that it can participate in the legal validity of electronic signatures.
7. **Electronic signature**: Unforgeability of electronic signatures must be assured.
8. **CAD**: Cryptographic keys used to authenticate an application to the TOE that acts on behalf of an authorized End User.

Subjects

Subjects	Definition
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory
S.Admin	User who is in charge to perform the TOE 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.

Note: In order to remain consistent with the underlying PP [17], the terms "Administrator" and "Signatory" are used throughout the rest of this document instead of "S.Admin" and "S.Signatory".

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**.

3.1 Assumptions

A.CGA *Trustworthy certification-generation application*

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA *Trustworthy signature-creation application*

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

3.2 Threats

T.Hack_Phys *Physical attacks through the TOE interfaces*

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

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

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

T.SCD_Derive *Derive the signature-creation data*

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

T.Sig_Forgery *Forgery of the electronic signature*

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

T.Sig_Repud *Repudiation of signatures*

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

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

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

T.DTBS_Forgery *Forgery of the DTBS-representation*

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

T.SigF_Misuse *Misuse of the signature-creation function of the TOE*

An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

3.3 Organisational security policies

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter 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 (according to directive Annex I) and is created by a SSCD.

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

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

OT.EMSEC_Design *Provide physical emanations security*

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

OT.Lifecycle_Security *Lifecycle security*

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

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

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

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify 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 of SVD that has been exported by that TOE.

OT.Tamper_ID *Tamper detection*

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

OT.Tamper_Resistance *Tamper resistance*

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

OT.Init SCD/SVD generation

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by 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 in configuration A shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS-representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

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

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

OT.Sig_Secure *Cryptographic security of the electronic signature*

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

4.2 Security objectives for the environment

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates qualified certificates which include inter alias

(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

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

5 IT Security Requirements

This chapter defines the security functional requirements and the security assurance requirements for the TOE and its environment. The chapter is organised as follows. Section 5.1 "TOE Security Functional Requirements" gives security functional requirements, Section 5.2 defines security assurance requirements for the TOE. Security requirements for TOE IT and non-IT environments are given in the Section 5.3 and the Section 5.4, respectively.

The requirements given in this Chapter are drawn from the Secure Signature-Creation Device (SSCD) Type 3 Protection Profile [17]. The requirements incorporate TOE-specific method and algorithms assignments.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA, RSA-PSS and specified cryptographic key sizes from 1280 bit up to 2048 bit that meet the following: Geeignete Krypto-Algorithmen gemäß §17(2) SigV [19]
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECC and specified cryptographic key sizes from 192 bit to 256 bit that meet the following: Geeignete Krypto-Algorithmen gemäß §17(2) SigV [19]

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

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

Application notes:

The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD/SVD pair is re-generated by the TOE. The TOE does not support re-generation of the SCD/SVD pair.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP_RSA	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm *generating and exporting a digital signature using the SCD and RSA Algorithm* and cryptographic key sizes from 1280 bit up to 2048 bit that meet the following: RSA or RSA-PSS and PKCS#1 v. 2.1 BT1 [21]
FCS_COP.1.1/ CORRESP_ECC	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm *generating and exporting a digital signature using the SCD and ECC-Algorithm* and cryptographic key sizes from 192 bit up to 256 bit that meet the following: ECDSA [22]

Application note:
SF5 SVD export and correspondence proof in section 6.1.5 contains further details about the correspondence proof.

FCS_COP.1.1/ SIGNING_RSA	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm RSA and SHA, and cryptographic key sizes 1280 bit up to 2048 bit that meet the following: (1) RSA or RSA-PSS and PKCS#1, v. 2.1 BT1 [21] (2) SHA-1, SHA-224, SHA 256: FIPS 180-2 [20]
FCS_COP.1.1/ SIGNING_ECC	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm ECC and SHA, and cryptographic key sizes 192 bit up to 256 bit that meet the following: (1) **The Elliptic Curve Digital Signature Algorithm** (ECDSA) [22] (2) SHA-1, SHA-224, SHA-256: FIPS 180-2 [20]
FCS_COP.1.1/SM	The TSF shall perform secure channel in accordance with a specified cryptographic algorithm (1) mutual device authentication and (2) key agreement with RSA, RSA-PSS or ECC, (3) Triple-DES encryption and decryption (4) Retail-MAC and cryptographic key sizes (1) 112 Bit Triple-DES and Retail-MAC (2) 1280 bit to 2048 bit RSA (3) 192 bit to 256 bit ECC that meet the following: (1) mutual device-authentication and key agreement according to DIN V66291-1 [23], Annex D (2) Triple-DES encryption and decryption: NIST SP 800-67 [24], (3) Retail-MAC: ANSI X9.19 [25].

Comment: the complementary parts to FCS_COP.1.1/SM are in sec. 5.3.1.3 FCS_COP.1.1/SM_CGA and 5.3.2.2 FCS_COP.1.1/SM_SCA).

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ SVD Transfer SFP	The TSF shall enforce the SVD Transfer SFP on export of SVD by User.
FDP_ACC.1.1/ Initialisation SFP	The TSF shall enforce the Initialisation SFP on generation of SCD/SVD pair by User.
FDP_ACC.1.1/ Personalisation SFP	The TSF shall enforce the Personalisation SFP on creation of RAD by Administrator.
FDP_ACC.1.1/Signature-creation SFP-ConfA	The TSF shall enforce the Signature-creation SFP-ConfA on 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are shown in the table below.

Table 5.1: Subjects, objects and attributes

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

Initialisation SFP

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.

SVD Transfer

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.

Personalisation SFP

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.

Signature-creation SFP-ConfA

FDP_ACF.1.1/Signature-creation SFP-ConfA	The TSF shall enforce the Signature-creation SFP-ConfA to objects based on General attribute and Signature-creation attribute group.
FDP_ACF.1.2/Signature-creation SFP-ConfA	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-ConfA	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/Signature-creation SFP-ConfA	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". **Refinement: (7.2)** (c) 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 "no". (d) User with the security attribute "role" set to "Administrator" is not allowed to create electronic signatures for any DTBS with SCD by the Signatory which security attribute "SCD operational" is set to any status.

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

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

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

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

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

FDP_ITC.1.1/DTBS-ConfA	The TSF shall enforce the Signature-creation SFP-ConfA when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2/DTBS-ConfA	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3/DTBS-ConfA	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: DTBS-representation shall be sent by an authorised SCA.

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

5.1.2.5 Subset residual information protection (FDP_RIP.1)

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

Note: The application of this TSFR is detailed in chapter 6, SF10 and in the rationale part in section 8.

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

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

1. SCD
2. RAD
3. SVD
4. CAD.

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

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

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

5.1.2.7 Data exchange integrity (FDP_UIT.1)

SVD Transfer

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.

Comment: the complementary part is in sec. 5.3.1.4, SVD Import

TOE DTBS

FDP_UIT.1.1/ TOE DTBS	The TSF shall enforce the Signature-creation SFP-ConfA 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.

Comment: the complementary part is in sec. 5.3.2.3, SCA DTBS.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1	The TSF shall detect when 10 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.

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1	The TSF shall allow (1) Identification of the user by means of TSF required by FIA_UID.1. (2) Establishing a trusted path between local user and the TOE by means of TSF required for the TOE by FTP_TRP.1/TOE-ConfA (3) Establishing a trusted channel between the SCA and the TOE by means of TSF required for the TOE by FTP_ITC.1/DTBS import-ConfA on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1	The TSF shall allow

(1) Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE-ConfA

(2) Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import-ConfA

on behalf of the user to be performed before the user is identified.

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1)

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

5.1.4.2 Management of security attributes (FMT_MSA.1)

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

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

5.1.4.3 Secure security attributes (FMT_MSA.2)

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

Application note: Security attributes are the key lengths for RSA and ECC keys.

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

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

Refinement

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

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

5.1.4.5 Management of TSF data (FMT_MTD.1)

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

5.1.4.6 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions[1]:

(a) Modifying the SCD/SVD management attribute
(b) Modifying the SCD operational attribute
(c) Creation of RAD
(d) Changing or unblocking of RAD
(e) Creation of CAD.

[1]Some of the management functions are not reflected by the TSFRs of section 5 but stated for completeness as they are introduced in the summary specification in section 6. This also helps to maintain consistency throughout the document.

Note: This is an additional element due to FI065.

5.1.4.7 Security roles (FMT_SMR.1)

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

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests at the request of an authorised user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.5.2 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit information via power consumption or EM radiation in excess of unintelligible limits enabling access to RAD, CAD and SCD.

FPT_EMSEC.1.2 The TSF shall ensure that S.User and S.OFFCARD are unable to use the following interface physical contacts of the smart card IC to gain access to RAD, CAD and SCD.

Application note:
The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate 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.

Obvious attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation**,** simple power analysis (SPA), differential power analysis (DPA), timing attacks, and in combination with active emission attacks.

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

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(a) Random number generation failures,
(b) Memory failures of different kind during cryptographic operations and TOE application execution,
(c) Errors caused by external effects: temperature or clock or voltage are out of range.

5.1.5.4 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.1.5.5 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist physical tampering scenarios: intrusion by physical, or mechanical means to the tamper responsive elements of the TOE ICC by responding automatically such that the TSP is not violated.

5.1.5.6 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up and at the conditions

1. Generation of SCD/SVD pair required by FCS_CKM.1.1/RSA
2. Generation of SCD/SVD pair required by FCS CKM.1.1/ECC
3. Signature-creation required by FCS_COP.1.1/SIGNING_RSA
4. Signature-creation required by FCS_COP.1.1/SIGNING_ECC

to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

SVD Transfer

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

FTP_ITC.1.2/ SVD Transfer The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

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

Comment: the complementary part is in sec. 5.3.1.5, SVD Import and 5.3.1.2, FCS_CKM.3.1/ CGA.

DTBS import

FTP_ITC.1.1/ DTBS import-ConfA 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-ConfA The TSF shall permit the **SCA** to initiate communication via the trusted channel.

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

Application Note:
The TOE shall support a trusted channel for receiving the DTBS and a trusted path for receiving the VAD with the SCA.

Comment: the complementary part is in sec. 5.3.2.4, SCA DTBS.

5.1.6.2 Trusted path (FTP_TRP.1)

FTP_TRP.1.1/ TOE-ConfA 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/ The TSF shall permit local users to initiate communication via the

TOE-ConfA	trusted path.
FTP_TRP.1.3/ TOE-ConfA	The TSF shall require the use of the trusted path for (1) initial user authentication, (2) to modify the RAD and (3) to unblock the RAD.

Comment: the complementary part is in sec. 5.3.2.5, SCA.

5.2 TOE Security Assurance Requirements

Table 5.2 Assurance Requirements: EAL(4) augmented (augmented requirements in bold)

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

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D	The developer shall use a CM system.
ACM_AUT.1.2D	The developer shall provide a CM plan.
ACM_AUT.1.1C	The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.
ACM_AUT.1.2C	The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3C	The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4C	The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D	The developer shall provide a reference for the TOE.
ACM_CAP.4.2D	The developer shall use a CM system.
ACM_CAP.4.3D	The developer shall provide CM documentation.
ACM_CAP.4.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C	The TOE shall be labelled with its reference.
ACM_CAP.4.3C	The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

Additional Element due to FI 003:

ACM_CAP.4.4Cnew	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6C	The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.4.7C	The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.8C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.9C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.4.12C	The CM system shall support the generation of the TOE.
ACM_CAP.4.13C	The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

Changed due to FI 004:

ACM_SCP.2.1D	The developer shall provide a list of configuration items for the TOE.

Changed due to FI 004 and 038:

ACM_SCP.2.1C	The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2D	The developer shall use the delivery procedures.
ADO_DEL.2.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2C	The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C	The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

Changes due to FI 051:

ADO_IGS.1.1C	The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1D	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D	The developer shall provide a functional specification.
ADV_FSP.2.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2C	The functional specification shall be internally consistent.
ADV_FSP.2.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4C	The functional specification shall completely represent the TSF.
ADV_FSP.2.5C	The functional specification shall include rationale that the TSF is completely represented.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D	The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1C	The presentation of the high-level design shall be informal.
ADV_HLD.2.2C	The high-level design shall be internally consistent.
ADV_HLD.2.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C	The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C	The high-level design shall identify which of the interfaces to the

subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3 Implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract

TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D	The developer shall provide a TSP model.
ADV_SPM.1.1C	The TSP model shall be informal.
ADV_SPM.1.2C	The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.2D	The developer shall demonstrate correspondence between the functional specification and the TSP model.
ADV_SPM.1.3C	The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled.
ADV_SPM.1.4C	The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D	The developer shall provide user guidance.
AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D	The developer shall produce development security documentation.
ALC_DVS.1.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1C	The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.1D	The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.1.2C	The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.2D	The developer shall provide life-cycle definition documentation.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1C	All development tools used for implementation shall be well-defined.
ALC_TAT.1.1D	The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2C	The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.1.2D	The developer shall document the selected implementation-dependent options of the development tools.
ALC_TAT.1.3C	The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.1D	The developer shall provide an analysis of the test coverage.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1C	The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1D	The developer shall provide the analysis of the depth of testing.

5.2.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D	The developer shall provide the TOE for testing.

ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Analysis and testing for insecure states (AVA_MSU.3)

AVA_MSU.3.1D	The developer shall provide guidance documentation.
AVA_MSU.3.2D	The developer shall document an analysis of the guidance documentation.
AVA_MSU.3.1C	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.3.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.3.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.3.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.3.5C	The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3 Highly resistant (AVA_VLA.4)

Changes due to FI 051:

AVA_VLA.4.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.4.2D	The developer shall provide vulnerability analysis documentation.

Changes due to FI 051:

AVA_VLA.4.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6C The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3 Security requirements for the IT environment

5.3.1 Certification generation application (CGA)

5.3.1.1 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1/ CGA The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method qualified certificate that meets the following: A relevant security policy of the Trust Centre.

Application note: It deals here with distribution of the certificates over SVD by the TC (trust center) (e.g. operating a directory service).

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following DIN V66291-1 [23], Annex D

Comment: the complementary part is in sec. 5.1.6.1, SVD Transfer.

5.3.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SM_CGA The TSF shall perform secure channel in accordance with a specified cryptographic algorithm
(1) mutual device authentication and
(2) key agreement with RSA, RSA-PSS or ECC,
(3) Triple-DES encryption and decryption
(4) Retail-MAC
and cryptographic key sizes
(1) 112 bit Triple-DES and Retail-MAC
(2) 1280 bit to 2048 bit RSA
(3) 192 bit to 256 bit ECC
that meet the following:
(1) mutual device-authentication and key agreement according to DIN V66291-1 [23], Annex D
(2) Triple-DES encryption and decryption according to NIST SP 800-67 [24],
(3) Retail-MAC: ANSI X9.19 [25].

Comment: the complementary part is in sec. 0, FCS_COP.1.1/SM.

5.3.1.4 Data exchange integrity (FDP_UIT.1)

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

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

Comment: the complementary part is in sec. 5.1.2.7, SVD Transfer.

5.3.1.5 Inter-TSF trusted channel (FTP_ITC.1)

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

Comment: the complementary part is in sec. 5.1.6.1, SVD Transfer.

5.3.2 Signature creation application (SCA)

5.3.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ SCA Hash	The TSF shall perform hashing the DTBS in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256 and cryptographic key sizes none that meets the following: FIPS 180-2 [20].

5.3.2.2 Signature creation application (SCA) supporting trusted path and trusted channel to the TOE

The SCA used for signature-creation with TOE shall support a trusted path for sending the VAD and a trusted channel for sending the DTBS.

FCS_COP.1.1/ SM_SCA	The TSF shall perform secure channel in accordance with a specified cryptographic algorithm (1) mutual device-authentication and (2) key agreement with RSA, RSA-PSS or ECC, (3) Triple-DES encryption and decryption (4) Retail-MAC and cryptographic key sizes (1) 112 bit Triple-DES and Retail-MAC (2) 1280 bit to 2048 bit RSA (3) 192 bit to 256 bit ECC that meet the following: (1) mutual device-authentication and key agreement according to DIN V66291-1 [23], Annex D, (2) Triple-DES encryption and decryption according to NIST SP 800-67[24], (3) Retail-MAC according to ANSI X9.19 [25].

Comment: The complementary part is in sec. 0, FCS_COP.1.1/SM.

5.3.2.3 Data exchange integrity (FDP_UIT.1)

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

SCA DTBS modification, deletion and insertion has occurred.
Comment: the complementary part is in sec. 5.1.2.7, TOE DTBS.

5.3.2.4 Inter-TSF trusted channel (FTP_ITC.1)

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

Comment: the complementary part is in sec. 5.1.6.1, DTBS Import-ConfA.

5.3.2.5 Trusted path (FTP_TRP.1)

FTP_TRP.1.1/ SCA	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ SCA	The TSF shall permit local users to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path for (1) usage of the human interface for authentication, (2) modification of the RAD and (3) transfer of DTBS to the TOE.

Comment: the complementary part is in sec. 5.1.6.2, TOE-ConfA.

5.4 Security Requirements for the Non-IT Environment

R.Administrator_Guide *Application of Administrator Guidance*

The implementation of the requirements of the Directive, ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (e), stipulates employees of the CSP or other relevant entities to follow the administrator guidance provided for the TOE. Appropriate supervision of the CSP or other relevant entities shall 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 [5], ANNEX II "Requirements for certification-service-providers issuing qualified certificates", literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

6 TOE Summary Specification

The TOE summary specification defines the instantiation of the security requirements for the TOE. The specification gives a description of all security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 TOE security functions

In order to meet the secure requirements, the TOE enforces the following ten security functions (SF):

SF1 Life cycle support,

SF2 Identification and Authentication of user,

SF3 Access control,

SF4 SCD/SVD pair generation,

SF5 SVD export and correspondence proof,

SF6 Signature creation,

SF7 Secure messaging,

SF8 Self test,

SF9 Physical protection,

SF10 Object reuse.

Each of the TOE security functions is described in the following sections in detail.

6.1.1 SF1 Life cycle support

The TOE life cycle defines states of manufacturing, testing, initialisation, completion, personalisation and destruction of the TOE. The TOE SF1 Life cycle support implements entity authentication and access control to TSF and other TOE functions designated for specific life cycle states only.

The TOE can be in one of the following states:

- "Initialization",
- Completion,
- Personalisation,
- Personalised,
- Terminated.

The TOE states are described in the following paragraphs of the section.

In the states "Initialization", Completion, and Personalisation the TOE user is the Administrator. In the state Personalised (i.e. during normal operation of the TOE) the TOE distinguishes between the Administrator and the Signatory (FMT_SMR.1) users. In the state Terminated, the life cycle of the TOE is terminated and no users are distinguished. The first three states are part of the development phase of figure 2 the last two states make up the operational phase in figure two.

State Initialization:

It is an initial state of the TOE that corresponds to a newly produced ICC after IC module implantation. In this state, a variety of tests (on ATR, ROM, RAM, EEPROM, RNG: FPT_AMT.1) is performed. The file system and other non-individual parameters such as necessary patch data are loaded to the TOE. The TOE leaves the "Initialization" state by execution of the LOAD_END command. The access control mechanism is not activated in this state[2]. Therefore, mutual authentication with the external equipment (CHECK ROMKEY command) using Triple-DES is mandatory to allow loading of data to the TOE. This state also allows certain tests to be performed.

[2] FDP_ACF.1 is not yet active

State Completion:

In this state, additional patch data, if necessary, is loaded to the card by execution of the LOAD COMPLETION DATA command. This command is secured by a Retail-MAC [25] calculated over the loaded data. The execution of LOAD COMPLETION DATA is only successful, if the MAC verification is successful. The access control mechanism is not yet activated in this state[3]. Upon successful execution of the COMPLETION END command, the files system is activated, and the TOE leaves the Completion state and is the "Personalisation" state.

Comment: This state is supported by the operating system but not used for the TOE, i. e. this state contains only the COMPLETION END command.

State Personalisation:

In this state, the personalisation data is loaded to the card. The access control mechanism is not yet activated in this state[4]. Therefore, the personalisation data loading can be secured by the secure messaging (this functionality is not implemented by SF1). The mutual device authentication must be successfully performed (ENABLE PERS command) in order to enable loading of the personalisation data. The SF1 enforces secure initial values for the SCD security attribute operational (FMT_MSA.3). Upon successful execution of the END PERS command, the TOE leaves the Personalisation state and is in the Personalised state.

State Personalised: In this state the access control mechanism and user commands are active. The TOE distinguishes between the Administrator and Signatory (FMT_SMR.1). The TOE provides the function to destroy the SCD (FCS_CKM.4) which is part of 6.1.10, SF10 Object Reuse, which finishes the live cycle of the TOE as SSCD, but the TOE remains operational as a smart card. The TOE offers no possibility to re-activate the SSCD functionality. Detected and handled permanent internal errors (FPT_FLS.1) transform the state Personalised into the state Terminated.

State Terminated: The state Terminated implements the secure failure state (FPT_FLS.1). The TOE sends an Error-ATR only and prohibits any other use of the TOE.

6.1.2 SF2 Identification and Authentication of user

The TSF SF2 Identification and Authentication of user (FMT_SMR.1) provides the following measures:

- SF2.1 Identification of user (FIA_UID.1),
- SF2.2 Authentication of user (FIA_UAU.1),
- SF2.3 Management of authentication information (FMT_MTD.1).

The TOE SF2.1 identifies users by means of

(1) selecting the respective cryptographic key of devices acting for the Administrator using the command MANAGE SECURITY ENVIRONMENT,

(2) selecting the Signature application which defines the PIN, PUK0 and PUK (FIA_ATD.1) to be used for the human user authentication.

The SF2.2 authenticates the identified user by means of

(1) commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE for the mutual device-SSCD authentication with respective authentication methods and respective cryptographic keys as CAD,

(2) command VERIFY implementing verification of the VAD with the PIN provided through secure messaging in combined mode, (FCS_COP.1/SM)

(3) command CHANGE REFERENCE DATA implementing the verification of the VAD with the selected PIN, or PUK0 provided through secure messaging in combined mode (FCS_COP.1/SM).

[3] FDP_ACF.1 is not yet active
[4] FDP_ACF.1 is not yet active

Commands INTERNAL AUTHENTICATE and EXTERNAL AUTHENTICATE will be used for mutual SSCD-device authentication of devices acting for the Administrator or the Signatory. The commands VERIFY and CHANGE REFERENCE DATA are designated for authentication of human users.

The SF2.3 provides management function and protection of authentication information by means of:

(1) creation of PIN, PUK0 and PUK as RAD (FMT_SMF.1),

(2) unlocking[5] and modification of the PIN by presenting PUK0 by means of the command CHANGE REFERENCE DATA,

(3) modification of a current PIN into a new PIN by means of the command CHANGE REFERENCE DATA, by presenting the PIN

(4) blocking of the PIN after 10 consecutive failed authentication attempts with the wrong PIN (FIA_AFL.1),

(5) blocking of the PUK0 or PUK after 3 consecutive failed authentication attempts with the wrong PUK0 or PUK (FIA_AFL.1),

(6) import of the cryptographic keys for authentication as CAD of an external device acting for the Administrator,

(7) the authentication information (VAD and RAD and CAD) is treated by the TOE in such a way that it cannot be disclosed by observing of the emanation of the TOE (FPT_EMSEC.1).

6.1.3 SF3 Access control

The TOE SF3 Access control implements

- SF3.1 Verification of access rights and
- SF3.2 Management of access rights.

The access control rights being described below depend on the current user role "Administrator" or "Signatory" (FMT_SMR.1).

The SF3.1 Verification of access rights controls the following TSF:

(1) creation of RAD and CAD (i.e. PIN, PUK, PUK0, cryptographic keys for authentication) which is only allowed for authenticated devices acting for the Administrator (FDP_ACC.1/ Personalisation, FDP_ACF.1/ Personalisation, FMT_SMF.1),

(2) unlocking and modifying the PIN by presenting of the PUK0 with the command CHANGE REFERENCE DATA which is only allowed for the Signatory (after successful verification with PUK) (FMT_MTD.1, FMT_SMF.1),

(3) modification of the PIN with command CHANGE REFERENCE DATA which is allowed only for the Signatory (after successful verification with the PIN) (FMT_MTD.1, FMT_SMF.1),

(4) unblocking the PIN with command RESET RETRY COUNTER which is allowed only for the Signatory (after successful verification with PUK) (FMT_MTD.1),

(5) setting the security attribute "SCD/SVD management" to "authorised" or "unauthorised" for Administrator and Signatory which is allowed only for Administrator (FMT_MSA.1/Administrator, FMT_SMF.1),

(6) generation of the SCD/SVD pair which is allowed only for Administrator or Signatory (see sec. 7.2) with security attribute "SCD/SVD management" set to "authorised" (FDP_ACC.1/Initialisation, FDP_ACF.1/Initialisation, FMT_SMF.1),

(7) setting the default-value of the security attribute "SCD operational" of the SCD to "no" which is allowed only for Administrator (FMT_MSA.3),

[5] the PIN will be activated

(8) modification of the security attribute "SCD operational" from "no" to "yes" which is allowed only for Signatory (FMT_MSA.1/Signatory, FMT_SMF.1),

(9) export of the SVD to the CGA which is allowed only for Administrator

(10) signature creation which is allowed only for Signatory for DTBS that (a) has been sent by an authorised SCA and (b) if security attribute "SCD operational" has been set to "yes" (FDP_ACC.1/Signature-Creation SFP-ConfA, FDP_ACF.1/Signature-Creation SFP-ConfA, and FMT_MOF.1).

For number (5) above the attribute is always set to "authorized" for the Administrator before the SCD/SVD pair is generated. After generation of the SCD/SVD pair by the Administrator this attribute is set to "not authorized". This means the Administrator is allowed to generate exactly one SCD/SVD pair. Therefore number (5) and number (6) limit key generation to the Administrator.

The SF3.2 Management of access rights implements

(1) setting the security attribute "SCD/SVD management" to "authorised" or "unauthorised" for Administrator and Signatory by Administrator,

(2) setting the default-value of the security attribute "SCD operational" of the SCD to "no".

(3) modification of the security attribute "SCD operational" of the SCD from "no" to "yes",

(4) setting the security attribute "sent by an authorised SCA" of DTBS (i) to "no" if the DTBS was not received through secure messaging and (ii) to "yes" if the DTBS was received through secure messaging.

For number (1) above see the explanation for number (5) of 6.1.3, SF3 Access control.

6.1.4 SF4 SCD/SVD pair generation

The TOE SF4 SCD/SVD pair generation generates SCD/SVD pairs as RSA key pairs with module length 1280 bit up to 2048 bit according to [19] or ECC key pairs with key length 192 bit up to 256 bit according to [19] (FCS_CKM.1/RSA, FCS_CKM.1/ECC, FMT_MSA.2). The SF4 uses the random number generator of the ICC. It implements countermeasures against attacks based on TOE emanation, SPA and timing attacks (FPT_EMSEC.1).

6.1.5 SF5 SVD export and correspondence proof

Remark: the verb "verify" OT.SCD_SVD_Corresp is to be understood as "assisting in proving". The verb "verify" is drawn from the Secure Signature-Creation Device (SSCD) Type 3 Protection Profile [17]. The understanding as stated here is necessary because not the TOE but a Trust Centre may need to verify the keys' correspondence. Due to this fact the verification by the TOE itself is senseless, but making the proof possible for a TC is the motivation of this objective.

For the SSCD to assist the CGA in verifying the correspondence of SVD the use of SCD is necessary but such use must not interfere with the signature directive [5]. Therefore the TOE provides the following two mechanisms that may be used by a CGA to verify the correspondence:

1. A signature where the Signatory signs a text (e. g. SVD) that is presented to her.
2. A technical signature where SCD is used to sign SVD without interaction with the Signatory[6].

Remark: Mechanism 1 and 2 have been chosen after consultation with the certification body (BSI) to find a PP-conformant[7] solution to the correspondence proof.
Mechnism 2 is a technical signature. In a strict technical sense also mechanism 1 is a technical signature in conjunction with the correspondence proof.
The CSP may choose which mechanism to use and may choose between:

1. Mechanism 1 which is implemented using SF6 Signature-creation e. g. over SVD.

[6] Such self-signatures are common in Public Key Infrastructures and imply no security risk if the underlying signature-creation algorithm(s) is secure.
[7] PP-conformance is necessary under the Austrian Signature law.

2. Mechanism 2: If mechanism 2 is chosen the self-signature with SCD over SVD is generated after issuing the command CORRESPONDENCE PROOF. Command CORRESPONDENCE PROOF then returns the signature of SVD with SCD.
3. Mechanisms 1 and 2 above.

If only mechanism 1 is chosen by the CGA because a technical signature that does not involve the Signatory is not admissible under country-specific regulations pertaining acknowledgement of signature creation devices command CORRESPONDENCE PROOF will be deactivated[8].
Correspondence proof is only allowed for Signatory in mechanism 1 and for Signatory and Administrator in mechanism 2.
By using mechanism 1 or 2 or both, described above, TOE SF5 creates and exports a digital signature with the SCD on demand (FCS_COP.1/CORRESP_RSA and FCS_COP.1/CORRESP_ECC). An external party can verify the validity of this signature by using the reference copy of the SVD stored at TC (CGA) during registration.

SVD export to CGA (TC) takes place after the key pair generation during the registration procedure. Only Administrator and Signatory are allowed to export SVD to the CGA (FDP_ACC.1 / SVD Transfer SFP, FDP_ACF.1 / SVD Transfer SFP, FDP_ETC.1 / SVD Transfer SFP) or any other entity in the IT-environment. The SVD generated is exported to a CGA over the secure channel by means of secure messaging (FDP_UIT.1 / SVD Transfer, FTP_ITC.1.1/ SVD Transfer).

6.1.6 SF6 Signature-creation

The TOE SF6 Signature-creation creates digital signatures for DTBS-representation received from SCA through secure messaging using the cryptographic algorithm RSA[9] or RSA-PSS [21] approved in [19] and cryptographic key sizes of 1280 up to 2048 bit as specified in [18] or the cryptographic algorithm ECDSA [22] approved in [19] and cryptographic key sizes of 192 bit up to 256 bit (FCS_COP.1/Signing_RSA, FCS_COP.1/Signing_ECC and FMT_MSA.2).

The DTBS-representation may be sent by the SCA to the TOE (FDP_ITC.1 / DTBS-ConfA, FDP_UIT.1 / TOE DTBS) as
(a) a hash-value of the DTBS by means of the command PSO PUT HASH or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS by means of the command PSO COMPUTE HASH in one or more steps or
(c) the DTBS by means of the command PSO COMPUTE HASH in one or more steps.
The hash value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE SF6 according to SHA-1, SHA-224, or SHA-256 [20] and is used as part of the digital signature input (DSI). The SF6 implements countermeasures against attacks based on TOE emanation (FPT_EMSEC.1), SPA, DPA, DFA and timing attacks. SF6 returns the computed digital signature to the SCA that sent the DTBS-representation. This is ensured through secure messaging.

6.1.7 SF7 Secure messaging

SF7 Secure messaging is always used to secure the communication with a CGA. TOE SF7 Secure messaging is always used to secure the communication with an SCA. Additionally, secure messaging is used to secure communications in State Personalisation of SF1

The TOE SF7 Secure messaging implements

- SF7.1 Management of SM keys (FMT_SMF.1),
- SF7. 2 Secure messaging communication

The SF7.1 Management of SM keys implements

In the operational state management of SM-keys implements

(1) import of public RSA or ECC keys for CV certificate verification of public RSA or ECC keys as CAD,

[8] The (dis-)allowance of a self-signature is currently under consideration. Forbiddance of a self-signature could only make sense for legal but not for technical reasons.
[9] Block type 01 as defined in [21] is used for padding.

(2) CV certificate verification and import of public RSA or ECC keys as CAD for device authentication of an external devices as agent of the administrator by means of command EXTERNAL AUTHENTICATE,

(3) import of RSA or ECC key pairs, storing the private key and export of the public key for mutual device authentication of the TOE by means of command EXTERNAL AUTHENTICATE

(4) selecting the key for establishing trusted path/channel (FTP_TRP.1/TOE-ConfA) using the command MANAGE SECURITY ENVIRONMENT.

For secure messaging in SF1 in State Personalisation SF7.1 Management of SM keys implements

(1) import of Triple-DES master keys used by key establishment methods and of Triple-DES authentication key used by the ENABLE_PERS (used for authentication in this state) command,

(2) SM session keys establishment according to ISO/IEC 11770-2.

The SF7.2 Secure messaging communication implements

In the operational state secure messaging communication implements

(1) mutual device authentication for establishing a session key according to DIN V66291-1,

(2) secure messaging in authentic mode according to ISO 7816-4 (FCS_COP.1 / SM),

(3) secure messaging in combined mode according to ISO 7816-4 (FCS_COP.1 / SM).

The SVD will be exported (FTP_ITC.1/SVD Transfer) and DTBS-representation will be imported (FTP_ITC.1/DTBS Import-ConfA) using SF7.

For secure messaging in SF1 in State Personalisation SF7.1 Secure messaging communication implements

(1) mutual device authentication according to ISO/IEC 9798-2 in combination with a session key establishment mechanism according to ISO/IEC 11770-2,

(2) secure messaging in protected mode according to ISO 7816-4,

(3) secure messaging in combined mode according to ISO 7816-4.

6.1.8 SF8 Self test

The TSF provides a suite of tests (FPT_AMT.1) executed upon a request of an authorised user. The tests are performed by means of the following commands:

(a) TEST_ROM command calculates the checksum over the ROM area enabling verification of the code located in ROM[10].

(b) TEST_RAM command performs a test of each RAM byte. In life-cycle "Personalized" this command is not available when the digital signature DF is selected.

(c) TEST_EEPROM command performs a test of each EEPROM byte from a memory area specified by the command parameters. The command is available in the state "Initialization" only.

(d) TEST_RANDOM command performs a RNG quality test. The test result is returned in the command response.

The TSF provides a suite of the following self tests (FPT_TST.1):

(a) Start-up tests like EEPROM before or after ATR,

(b) TRNG-Test before key generation,

(c) special tests implementing FDP_SDI.2 / Persistent and FDP_SDI.2 / DTBS.

[10] In life-cycle state „Personalized" this command is not available.

If any of the above self tests has failed, the TOE will enter its secure state (FPT_FLS.1).

FDP_SDI.2/Persistent comprises integrity checks for SCD, SVD, RAD and CAD which can be seen not only as User data but may also be considered as being TSF data and therefore covers FPT_TST.1.2 As FDP_SDI.2 has been taken over from the PP for SCD, SVD and RAD and CAD has been added to distinguish between reference authentication data for the Signatory (RAD) and for the Administrator (CAD) it is assumed that also the PP authors had the opinion that this data is TSF Data as well as user data. As user data is checked and an error returned if the integrity has been lost or compromised using such data implicitly supplies a verification of the data. To cover FPT_TST.1.3 it has to be observed that manipulation of executable code located in ROM implies changing the contents of parts of the ROM which as the name "Read Only Memory" implies is not possible. Additionally, the IC encrypts the ROM content and addresses using a block cipher using a key that is unique for every ROM code. Moreover, the IC checks the integrity of the ROM code during every fetching or reading of ROM memory and triggers a reset if the integrity check fails. Any technology that would allow changing the contents of the ROM would most likely imply that an adversary using such technology could compromise the TOE totally. Therefore executable code located in ROM does not need to be user verifiable on demand. For executable code that is located in the EEPROM a test of the integrity of this code is always performed on start-up of the TOE which implicitly covers FPT_TST.1.3 because in case of an unsuccessful integrity check the TOE enters its secure state. Additionally, the EEPROM contains circuitry the checks the integrity of every byte and is able to correct one bit errors per byte.

6.1.9 SF9 Physical protection

TOE implements the security function SF9 that resists physical tampering. The TOE hardware detects the physical tampering (FPT_PHP.1) and reports this to the TOE software reacting to this automatically such that the assets are not violated (FPT_PHP.3).

6.1.10 SF10 Object Reuse

TOE implements the security function SF10 that ensures an active destruction of sensitive objects, if they are not being used any more.

SF10 actively destructs (i) SCD or/and (ii) parts of SCD as well as VAD, RAD and CAD *temporarily* stored in RAM or EEPROM of the TOE immediately after their use (FDP_RIP.1).

SF10 actively destructs SCD *persistently* stored in the TOE if they are not being used any more (FCS_CKM.4) by destruction of SCD which may be enforced by the DELETE KEY command.

6.1.11 SOF claim

According to the CEM [4] a Security Target shall identify all mechanisms which can be assessed according to the assurance requirement AVA_SOF.1.

The following mechanisms contributing to these functions were identified, which can be analysed for their permutational or probabilistic properties:

- The PIN/PUK0/PUK mechanism can be analysed with probabilistic methods.
- The used checksum mechanisms can be analysed using probabilistic methods.
- The PRNG can be analysed using probabilistic methods.
- Some of the physical protection mechanisms of the underlying IC can be analysed using probabilistic or permutational methods
- XOR-masking of keys

Therefore an explicit SOF claim of "high" is made for these mechanisms. Table 6.1 shows the correspondence of the identified functions and the defined security functions SF1-SF10, including the SOF claim.

Note: The cryptographic algorithms used by the TOE can also be analysed with permutational or probabilistic methods, but this is not in the scope of CC evaluations.

Table 6.1: Security functions and and probabilistic/permutational mechanisms

		PIN/PUK0/PUK	Checksum Mech.	XOR-masking of keys	PRNG	Physical protection	SOF Claim
SF1	Life cycle support		X				
SF2	Ident. and Auth. of user	X	X		X		SOF-high
SF3	Access control		X				SOF-high
SF4	SCD/SVD pair generation		X		X		SOF-high
SF5	SVD exp. and corresp. proof		X				
SF6	Signature-creation		X		X		SOF-high
SF7	Secure Messaging		X		X		SOF-high
SF8	Self test		X	X			SOF-high
SF9	Physical Protection					X	SOF-high
SF10	Object Reuse						

Remark: The PRNG is only used for SF6, Signature-creation in case of ECDSA [22]. Refinements in more specific documents of the ADV family may add security functions, especially for checksum mechanisms. XOR-masking of key material is not mandatory according to this ST or the underlying PP but directly supports OT.SCD_Secrecy.

6.2 Assurance measures

TOE implements the assurance measures exactly drawn from the assurance requirements defined in sec. 5.2. Naming of each assurance measure is derived from the name of the according assurance requirement.

TOE implements the following assurance measures by providing the appropriate documents and activities:

Table 6.2: TOE Assurance Measures

Assurance Measures	remarks
ACM_AUT.1M	configuration management documentation
ACM_CAP.4M	configuration management documentation
ACM_SCP.2M	configuration management documentation
ADO_DEL.2M	parts of delivery documentation
ADO_IGS.1M	secure installation, generation and start-up procedures
ADV_FSP.2M	fully defined external interfaces
ADV_HLD.2M	high-level design (security enforcing)
ADV_IMP.1M	subset of the implementation of the TSF
ADV_LLD.1M	descriptive low-level design
ADV_RCR.1M	correspondence analysis between

	• TOE summary specification and fully defined external interfaces, • functional specification and high-level design, • high-level design and low-level design and • low-level design and implementation representation.
ADV_SPM.1M	(informal) TSP model
AGD_ADM.1M	administrator guidance
AGD_USR.1M	user guidance
ALC_DVS.1M	development security documentation
ALC_LCD.1M	life cycle definition document
ALC_TAT.1M	development tools documentation
ATE_COV.2M	test coverage analysis
ATE_DPT.1M	depth of testing analysis
ATE_FUN.1M	test documentation
ATE_IND.2M	
AVA_MSU.3M	administrator and user guidance, misuse analysis
AVA_SOF.1M	strength of function claims analysis
AVA_VLA.4M	vulnarability assessment

7 PP claims

7.1 PP reference

The ST is compliant to the PP SSCD Type 3 [17].

7.2 PP refinements

The following refinements have been made to the PP:

The SFR FDP_ACF.1/Signature-creation SFP-ConfA has been refined for reasons of completeness. The added topic (c) in the element FDP_ACF.1.4/Signature-creation SFP-ConfA strengthens the SFP and leads to an unambiguous formulation. For this the refinement constitutes a stronger SFR and leads to no security loophole.

The application note in 5.1.1.2 Cryptographic key destruction (FCS_CKM.4) has been adjusted to exclude re-generation of SCD/SVD pair. Inclusion of this provision does not affect the possibility to destruct the SCD/SVD pair on demand of the Signatory or Administrator and leads to no security loopholes. Additionally, it simplifies the administration of the TOE which allows for easier assessment of the TOE.

7.3 PP additions

The following Security Objectives and IT-Security Requirements are additionally included into the current Security Target:

None.

TOE-Functional Security Requirements:

FCS_COP.1.1/SM

The TSFR FCS_COP.1.1/SM requires that the TOE supports an asymmetric session-key protocol and describes the cryptographic details for establishing the secure messaging.

The "Common Criteria, Part 2: Security functional requirements, August 2005, Version 2.3", [2], includes one applicable interpretation in the definition of the TSFRs. This mandatory and official Final Interpretation (FI) is incorporated in this Security Target.

The following TSFR is affected:

FMT_SMF FI065: one new family

Security Assurance requirements

The "Common Criteria, Part 3: Security assurance requirements, August 2005, Version 2.3", [3], includes some changes in the definition of the SARs. These mandatory and official Final Interpretations (FI) are incorporated in this Security Target.

The following SARs are affected:

ACM_CAP.4 FI003: one new element

ACM_SCP.2 FI004 and FI038: completely reformulated

ADO_IGS.1 FI051: one new element

AVA_VLA.4 FI051: completely reformulated

Functional Security Requirements for the IT-Environment:

FCS_COP.1.1/SM_CGA

FCS_COP.1.1/SM_SCA

These objects of the current security policy are clearly identified and defined in the relevant sections of this document.

8 Rationale

8.1 Security objectives rationale

8.1.1 Security Objectives Coverage

Table 8.1-: Security Environment to Security Objectives Mapping

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

8.1.2 Security Objectives Sufficiency

8.1.2.1 Policies and Security Objective Sufficiency

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

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [5], article 5, paragraph 1. Directive [5], 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 and guarantees its secrecy. This is addressed by OT.Sigy_SigF and OT.SCD_Secrecy ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. OT.Init provides that generation of the SCD/SVD pair is restricted to authorised users.

8.1.2.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. Physical

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

T.SCD_Divulg (Storing,copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [5], recital (18). This threat is countered by OT.SCD_Secrecy which assures the secrecy of the SCD used for signature generation.

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

T.DTBS_Forgery (Forgery of the DTBS-representation) addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which 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_Intend.

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 [5], Annex III, paragraph 1, literal (c). This threat is addressed by the OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OE.SCA_Data_Intend (Data intended to be signed), OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity), and OE.HI_VAD (Protection of the VAD) as follows: OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate signatory only. OE.SCA_Data_Intend ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of OT.DTBS_Integrity_TOE and OE.SCA_Data_Intend counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, OE.HI_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed.

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

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

T.Sig_Repud (Repudiation of electronic signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by OE.CGA_QCert (Generation of qualified certificates), OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD), OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD), OT.SCD_SVD_Corresp (Correspondence between SVD and SCD), OT.SCD_Unique (Uniqueness of the signature-creation data), OT.SCD_Secrecy (Secrecy of the

signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection), OT.Tamper_Resistance (Tamper resistance), OT.Lifecycle_Security (Lifecycle security), OT.Sigy_SigF (Signature generation function for the legitimate signatory only), OT.Sig_Secure (Cryptographic security of the electronic signature), OE.SCA_Data_Intend (SCA sends representation of data intended to be signed) and OT.DTBS_Integrity_TOE (Verification of the DTBS-representation integrity).

OE.CGA_QCert ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. OE.CGA_QCert, OT.SVD_Auth_TOE and OE.SVD_Auth_CGA ensure the integrity of the SVD. OE.CGA_QCert and OT.SCD_SVD_Corresp ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. 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.

8.1.2.3 Assumptions and Security Objective Sufficiency

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

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

8.2 Security requirements rationale

8.2.1 Security Requirement Coverage

Table 8.2 : Functional Requirement to TOE Security Objective Mapping

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_CKM.1/RSA				x	x				x			
FCS_CKM.1/ECC				x	x				x			
FCS_CKM.4		x		x								
FCS_COP.1/CORRESP_RSA					x							
FCS_COP.1/CORRESP_ECC					x							

TOE Security Functional Requirement / TOE Security objectives	OT.EMSEC_Design	OT.lifecycle_Security	OT.Init	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SVD_Auth_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure
FCS_COP.1/SIGNING_RSA												x
FCS_COP.1/SIGNING_ECC												x
FCS_COP.1/SM						x				x		
FDP_ACC.1/SVD TRANSFER SFP						x						
FDP_ACC.1/INITIALISATION SFP			x	x								
FDP_ACC.1/PERSONALISATION SFP											x	
FDP_ACC.1/SIGNATURE-CREATION SFP-ConfA										x	x	
FDP_ACF.1/INITIALISATION SFP			x	x								
FDP_ACF.1/SVD TRANSFER SFP						x						
FDP_ACF.1/PERSONALISATION SFP											x	
FDP_ACF.1/SIGNATURE-CREATION SFP-ConfA										x	x	
FDP_ETC.1/SVD TRANSFER						x						
FDP_ITC.1/DTBS-ConfA										x		
FDP_RIP.1				x							x	
FDP_SDI.2/Persistent				x	x						x	x
FDP_SDI.2/DTBS										x		
FDP_UIT.1/SVD TRANSFER						x						
FDP_UIT.1/TOE DTBS										x		
FIA_AFL.1			x								x	
FIA_ATD.1			x								x	
FIA_UAU.1			x								x	
FIA_UID.1			x								x	
FMT_MOF.1				x							x	
FMT_MSA.1/ADMINISTRATOR			x	x								
FMT_MSA.1/SIGNATORY											x	
FMT_MSA.2											x	
FMT_MSA.3			x	x							x	
FMT_MTD.1											x	
FMT_SMF.1			x	x							x	
FMT_SMR.1				x							x	
FPT_AMT.1		x		x								x
FPT_EMSEC.1	x											
FPT_FLS.1				x				x				
FPT_PHP.1							x					
FPT_PHP.3								x				
FPT_TST.1		x										x
FTP_ITC.1/SVD TRANSFER						x						
FTP_ITC.1/DTBS IMPORT-ConfA										x		
FTP_TRP.1/TOE-ConfA											x	

Table 8.3 : IT Environment Functional requirements to Environment Security Objective Mapping

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

Table 8.4: Assurances Requirement to Security Objective Mapping

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

8.2.2 Security Requirements Sufficiency

8.2.2.1 TOE Security Requirements Sufficiency

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

OT.Init (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. FIA_ATD.1 defines RAD and CAD 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 using appropriate management functions of FMT_SMF.1. Access control is provided by FDP_ACC.1/INITIALISATION SFP and FDP_ACF.1/INITIALISATION SFP. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Security (Lifecycle security) is provided by the security assurance requirements ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ADO_DEL.2, and ADO_IGS.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions FPT_TST.1

and FPT_AMT.1 provide failure detection throughout the lifecycle. FCS_CKM.4 provides secure destruction of the SCD.

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

The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used 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. FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECC chosen according to [19] ensure the cryptographic quality of SCD/SVD.

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

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

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

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [5], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1/RSA and FCS_CKM.1/ECC.

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 FCS_COP.1/SM, FDP_ITC.1/DTBS-ConfA, FTP_ITC.1/DTBS IMPORT-ConfA, and by FDP_UIT.1/TOE DTBS. The access control requirements of FDP_ACC.1/SIGNATURE CREATION SFP-ConfA and FDP_ACF.1/SIGNATURE CREATION SFP-ConfA keep unauthorised parties off from altering the DTBS-representation.

The verification that the DTBS-representation has not been altered by the TOE is done by integrity functions specified by FDP_SDI.2/DTBS.

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

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

The security functions specified by FIA_ATD.1, FMT_MOF.1, FMT_MSA.2, FMT_MSA.3 and FMT_SMF.1 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 function specified by FDP_SDI.2 ensures the integrity of stored data while stored. The integrity (and also the confidentiality) of the stored data during communication is ensured by the security function specified by FTP_TRP.1/TOE-ConfA.

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

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

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

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

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

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks. FPT_FLS.1 preserves a secure state in occurrence of a failure caused by external effects.

8.2.2.2 TOE Environment Security Requirements Sufficiency

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

OE.HI_VAD (Protection of the VAD) covers confidentiality and integrity of the VAD, which is provided by the trusted path FTP_TRP.1/SCA by secure messaging FCS_COP.1/SM_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. The implementation by secure messaging is provided by FCS_COP.1/SM_SCA.

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD IMPORT, which guarantees it's integrity by establishing a trusted channel using FCS_COP.1/SM_CGA.

8.3 Dependency Rationale

8.3.1 Functional and Assurance Requirements Dependencies

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

Table 8.5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies

Requirement	Dependencies
Functional Requirements for the TOE	
FCS_CKM.1/RSA	FCS_COP.1/SIGNING_RSA, FCS_CKM.4, FMT_MSA.2
FCS_CKM.1/ECC	FCS_COP.1/SIGNING_ECC, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1/RSA and FCS_CKM.1/ECC, FMT_MSA.2
FCS_COP.1/ CORRESP_RSA	FDP_ITC.1/DTBS-ConfA, FCS_CKM.1/RSA, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ CORRESP_ECC	FDP_ITC.1/DTBS-ConfA FCS_CKM.1/ECC, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING_RSA	FDP_ITC.1/DTBS-ConfA, FCS_CKM.1/RSA, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING_ECC	FDP_ITC.1/DTBS-ConfA, FCS_CKM.1/ECC, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SM	FDP_ITC.1/DTBS-ConfA, FCS_CKM.1/RSA and FCS_CKM.1/ECC, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1/ Initialisation SFP	FDP_ACF.1/Initialisation SFP
FDP_ACC.1/ Personalisation SFP	FDP_ACF.1/Personalisation SFP
FDP_ACC.1/ Signature-Creation SFP-ConfA	FDP_ACF.1/Signature Creation SFP-ConfA
FDP_ACC.1/ SVD Transfer SFP	FDP_ACF.1/SVD Transfer SFP
FDP_ACF.1/ Initialisation SFP	FDP_ACC.1/Initialisation SFP, FMT_MSA.3
FDP_ACF.1/ Personalisation SFP	FDP_ACC.1/Personalisation SFP, FMT_MSA.3
FDP_ACF.1/ Signature-Creation SFP-ConfA	FDP_ACC.1/Signature-Creation SFP-ConfA, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/DTBS-ConfA	FDP_ACC.1/ Signature-Creation SFP-ConfA, FMT_MSA.3
FDP_UIT.1/ SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP

Requirement	Dependencies
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/Signature_Creation SFP-ConfA, FTP_ITC.1/DTBS Import-ConfA,
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1 (FI 065)
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1, FMT_SMF.1 (FI 065)
FMT_MSA.1/Signatory	FDP_ACC.1/Signature Creation SFP-ConfA, FMT_SMR.1, FMT_SMF.1 (FI 065)
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_SMR.1, FMT_SMF.1 (FI 065)
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	(**FI 212:** ~~FMT_MOF.1)~~
FPT_TST.1	FPT_AMT.1
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	(**FI 095:** ~~ACM_SCP.1)~~, ALC_DVS.1
ACM_SCP.2	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.3	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1
Functional Requirements for Certification generation application (CGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 8.3.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 8.3.2 for justification
FDP_UIT.1/ SVD IMPORT	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see sub-section 8.3.2 for justification

Requirement	Dependencies
FTP_ITC.1/ SVD IMPORT	None
FCS_COP.1/ SM_CGA	unsupported dependencies, see sub-section 8.3.2 for justification)
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see sub-section 8.3.2 for justification
FDP_UIT.1/ SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 8.3.2 for justification
FTP_ITC.1/ SCA DTBS	None
FTP_TRP.1/SCA	None
FCS_COP.1/ SM_SCA	unsupported dependencies, see sub-section 8.3.2 for justification)

8.3.2 Justification of Unsupported Dependencies

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

FCS_CKM.2/ CGA	The CGA generates qualified electronic signatures including the SVD imported from the TOE. The FCS_CKM.1/RSA and FCS_CKM.1/ECC are not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted channel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1/RSA and FCS_CKM.1/ECC are not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this ST.
FDP_UIT.1/ SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this ST.
FCS_COP.1/ SM_CGA	Any key or security management for the CGA are outside of the scope of this ST. Therefore FDP_ITC.1, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FCS_CKM.4 and FMT_MSA.2 are not considered here.
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/RSA, FCS_CKM.1/ECC, FCS_CKM.4 and FMT_MSA.2 are not required for FCS_COP.1/SCA HASH in the SCA.
FDP_UIT.1/ SCA DTBS	Access control (FDP_ACC.1.1) for the SCA are outside of the scope of this ST.
FCS_COP.1/ SM_SCA	Any key or security management for the SCA are outside of the scope of this ST. Therefore FDP_ITC.1, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FCS_CKM.4 and FMT_MSA.2 are not considered here.

8.4 Security Requirements Grounding in Objectives

This chapter covers the groundings that have not been done in the precedent chapter.

Table 8.6: Assurance Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4

ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.1	EAL 4
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.1	EAL4, OT.Lifecycle_Security
ALC_LCD.1	EAL4, OT.Lifecycle_Security
ALC_TAT.1	EAL4, OT.Lifecycle_Security
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	OT.Sigy_SigF
AVA_SOF.1	EAL 4, OT.SCD_Secrecy, OT.Sigy_SigF
AVA_VLA.4	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

8.5 TOE summary specification rationale

8.5.1 Security Function Coverage

Table 8.7: TOE security function to TOE security functional requirement mapping

TOE Security Functional Requirements/TOE Security Functions	SF 1 Life cycle support	SF 2 Identification and Authentication of user	SF 3 Access control	SF 4 SCD/SVD pair generation	SF 5 SVD export and correspondence proof	SF 6 Signature-creation	SF 7 Secure messaging	SF 8 Self test	SF 9 Physical protection	SF 10 Object Reuse
FCS_CKM.1/RSA				**x**						
FCS_CKM.1/ECC				**x**						
FCS_CKM.4										**x**
FCS_COP.1 / CORRESP_RSA					**x**					
FCS_COP.1 / CORRESP_ECC					**x**					
FCS_COP.1 / SIGNING_RSA						**x**				
FCS_COP.1 / SIGNING_ECC						**x**				
FCS_COP.1 / SM		**x**					**x**			
FDP_ACC.1 / Initialisation SFP			**x**							
FDP_ACC.1 / Personalisation SFP			**x**							
FDP_ACC.1 / Signature-Creation SFP-			**x**							

TOE Security Functional Requirements/TOE Security Functions	SF 1 Life cycle support	SF 2 Identification and Authentication of user	SF 3 Access control	SF 4 SCD/SVD pair generation	SF 5 SVD export and correspondence proof	SF 6 Signature-creation	SF 7 Secure messaging	SF 8 Self test	SF 9 Physical protection	SF 10 Object Reuse
ConfA										
FDP_ACC.1 / SVD Transfer SFP					x					
FDP_ACF.1 / Initialisation SFP			x							
FDP_ACF.1 / Personalisation SFP			x							
FDP_ACF.1 / Signature-Creation SFP-ConfA			x							
FDP_ACF.1 / SVD Transfer SFP					x					
FDP_ETC.1 / SVD Transfer SFP					x					
FDP_ITC.1 / DTBS_ConfA						x				
FDP_RIP.1										x
FDP_SDI.2 / Persistent								x		
FDP_SDI.2 / DTBS								x		
FDP_UIT.1 / SVD Transfer					x					
FDP_UIT.1 / TOE DTBS						x				
FIA_AFL.1		x								
FIA_ATD.1		x								
FIA_UAU.1		x								
FIA_UID.1		x								
FMT_MOF.1			x							
FMT_MSA.1 / Administrator			x							
FMT_MSA.1 / Signatory			x							
FMT_MSA.2				x		x				
FMT_MSA.3	x		x							
FMT_MTD.1		x	x							
FMT_SMF.1		x	x				x			
FMT_SMR.1	x	x	x							
FPT_AMT.1	x							x		
FPT_EMSEC.1		x		x		x				
FPT_FLS.1	x							x		
FPT_PHP.1									x	
FPT_PHP.3									x	
FPT_TST.1								x		
FTP_ITC.1 / SVD_Transfer					x		x			
FTP_ITC.1 / DTBS_Import-$Conf_A$							x			
FTP_TRP.1 / TOE-$Conf_A$							x			

This table has a formal character.

8.5.2 TOE Security Function Sufficiency

Each TOE security functional requirement is implemented by at least one security function. How and whether the security functions actually implement the TOE security functional requirement is described in sec. 6.1.

8.5.3 Assurance measures rationale

Table 8.8: Mapping TOE Assurance Requirements to TOE Assurance Measures

TOE Security Assurance Requirements	TOE Assurance Measures
ACM_AUT.1	ACM_AUT.1M
ACM_CAP.4	ACM_CAP.4M
ACM_SCP.2	ACM_SCP.2M
ADO_DEL.2	ADO_DEL.2M
ADO_IGS.1	ADO_IGS.1M
ADV_FSP.2	ADV_FSP.2M
ADV_HLD.2	ADV_HLD.2M
ADV_IMP.1	ADV_IMP.1M
ADV_LLD.1	ADV_LLD.1M
ADV_RCR.1	ADV_RCR.1M
ADV_SPM.1	ADV_SPM.1M
AGD_ADM.1	AGD_ADM.1M
AGD_USR.1	AGD_USR.1M
ALC_DVS.1	ALC_DVS.1M
ALC_LCD.1	ALC_LCD.1M
ALC_TAT.1	ALC_TAT.1M
ATE_COV.2	ATE_COV.2M
ATE_DPT.1	ATE_DPT.1M
ATE_FUN.1	ATE_FUN.1M
ATE_IND.2	ATE_IND.2M
AVA_MSU.3	AVA_MSU.3M
AVA_SOF.1	AVA_SOF.1M
AVA_VLA.4	AVA_VLA.4M

Each TOE security assurance requirement is implemented by exactly one assurance measure. The content and application of these assurance measures exactly accords with the assurance components of CC part 3 [3] with the same identifier, respectively, and CEM [4].

8.5.4 Mutual supportiveness of the Security Functions

The TOE security functions are mutual supportive.

Life cycle support (SF1) needs mutual authentication including (SF7) secure messaging for sensitive data in the state "Personalisation". Administrator access is provided by the user identification and authentication (SF2). Changing to State "Terminated" can be caused by physical protection (SF9). Self tests in "Virginal" state need the test functions (SF8) and destruction of SVD need the object reuse functions (SF10).

The identification and authentication of user (SF2) needs secure messaging (SF7) for VAD import.

The access control functions (SF3) are based on the user identification and authentication (SF2) and the life cycle support (SF1). The import of the DTBS and the export of the SVD to the CGA are using secure messaging (SF7). In the last case the SVD export functions (SF5) are also needed.

The export of the SVD (SF5) uses secure messaging functions (SF7).

The signature creation (SF6) is subjected to the access control functions (SF3).

This context is represented in the following table:

Table 8.9: Mutual supportiveness of the security functions.

	Function		uses function(s)
SF1	State "Personalisation" needs mutual authentication including SM	SF7	Secure messaging
		SF2	User identification and authentication
	Test functions in "Virginal" state	SF8	Self tests
	Switching to state "Terminated"	SF9	Physical Protection
	Destruction of SCD	SF10	Object Reuse
SF2	VERIFY and CHANGE REFERENCE DATA in combined mode	SF7	Secure messaging in combined mode
SF3	User dependent access control	SF2	User identification and authentication
		SF1	Life cycle "Completion"/"Personalised"
	Export SVD to CGA	SF7 SF5	Secure messaging SVD export
	Import of DTBS	SF7	Secure messaging
SF5	SVD export	SF7	Secure messaging
SF6	Import of DTBS	SF7	Secure messaging
	Signature creation	SF3	Access control

8.6 Rationale for Extensions

The additional family FPT_EMSEC TOE Emanation of the Class FPT Protection of the TSF is defined in the SSCD PP [17] to which the ST claims conformance. The ST does not use other extensions to the CC part 2 [2].

8.7 Rationale for Assurance Level 4 Augmented

The assurance level for this security target is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this security target is just such a product. Augmentation results from the selection of:

AVA_MSU.3 Vulnerability Assessment - Misuse - Analysis and testing for insecure states
AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

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

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

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

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

AVA_VLA.4 Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. AVA_VLA.4 has the following dependencies:

ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

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

8.8 Rationale for Strength of Function High

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

8.9 PP claims rationale

The PP claims rationale statement shall explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

The necessary rationales are given in 7.2 for the PP refinements and in 7.3 for the PP additions.

9 Glossary

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

Advanced electronic signature (defined in the Directive [5], article 2.2) means an electronic signature which meets the following requirements:

(d) it is uniquely linked to the signatory;
(e) it is capable of identifying the signatory;
(f) it is created using means that the signatory can maintain under his sole control, and
(g) 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.

Authorised SCA means a signature creation application, which is able to establish a trusted path/channel as required by the TSF in configuration A. The requirements for the environment in configuration B ensure that the signature creation application is authorised.

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [5], 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
(d) the SSCD proof of correspondence between SCD and SVD and
(e) 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 [5], article 2.11)

Cryptographic authentication data (CAD) means cryptographic keys used to authenticate an application to the TOE that acts on behalf of an authorized user.

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 (b) or the hash-value in case (c) 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 [5] is also referred to as the 'Directive' in the remainder of the PP.

Digital signature input are the data on which the cryptographic signature algorithm (for the TOE the RSA-algorithm) is applied.

List of approved algorithms and parameters document describing approved cryptographic algorithms together with the requirements on their parameters and published by the Algorithms group working under the umbrella of European Electronic Signature Standardisation Initiative Steering Group [18] for approvement by the Article 9 committee.

Normal-PIN is a special case of the PIN consisting of 6, 7 or 8 digits.

PIN is a part of the SRAD which is whether a Transport-PIN or a Normal-PIN.

PUK is a part of the SRAD consisting of 6, 7 or 8 digits.

Qualified certificate means a certificate, which meets the requirements laid down in Annex I of the Directive [5] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [5]. (defined in the Directive [5], 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 [5], 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 [5]. (SSCD is defined in the Directive [5], 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 [5], 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
(f) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision,
(g) to send a DTBS-representation to the TOE, if the signatory indicates by specific non-misinterpretable input or action the intend to sign,
(h) 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 [5], 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 [5], 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.

Transport-PIN is a special case of the PIN consisting of 5 digits.

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.

10 Abbreviations

Acronym	Meaning
CAD	Cryptographic authentication data
CGA	Certification generation application
CSP	Certification-service-provider
DPA	Differential Power Analysis, an attack, which may compromise cryptographic keys by analysing the power consumption of the smart card chip.
DSI	digital signature input
DTBS	Data to be signed
EAL	Evaluation assurance level
FSP	Functional Specification
HLD	High-level design
IC	Integrated Circuit
ICC	Integrated Circuit Card
OE	Security objective for the environment
OT	Security objective for the TOE
PIN	Personal identification number
PUK	Personal unblock key
PP	Protection profile
RAD	Reference authentication data
SAR	Security Assurance Requirement
SCA	Signature-creation application
SCD	Signature-creation data
SCS	Signature-creation system
SF	Security Function
SFP	Security function policy
SFR	Security Functional Requirement
SigG	Signatur Gesetz
SigV	Signatur Verordnung
SOF	Strength of function
SSCD	Secure signature-creation device
SSM	Sicherheitsspezifische Mechanismen
ST	Security Target
SVAD	signatory's verification authentication data
SVD	Signature verification data
SW	Software

Tab.	Table(s)
TC	Trust Center
TOE	Target of Evaluation
TSC	TSF scope of control
TSF	TOE security functions
TSFI	TOE security functions interface
TSP	TOE security policy
VAD	Verification authentication data

11 Bibliography

Laws, standards

[1] Common Criteria, Part 1: Introduction and general model, August 2005, Version 2.3, CCMB-2005-08-001

[2] Common Criteria, Part 2: Security functional requirements, August 2005, Version 2.3, CCMB-2005-08-002

[3] Common Criteria, Part 3: Security assurance requirements, August 2005, Version 2.3, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, August 2005, Version 2.3, CCMB-2005-08-004

[5] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[6] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG) (inkl. Einarbeitung der Novelle lt. Ministerrat 10/2000), 19. August 1999, BGBl. I Nr. 190/1999

[7] Signaturgesetz 1. Novelle, 29. Dezember 2000, BGBl. I Nr. 137/2000

[8] Signaturgesetz 2. Novelle, 30. März 2001, BGBl. I Nr. 32/2001 Artikel VII

[9] Signaturgesetz 3. Novelle, 21. Dezember 2001, BGBl. I Nr. 152/2001 Artikel II

[10] Signaturgesetz 4. Novelle, 7. Jänner 2008, BGBl. I Nr. 8/2008 Artikel 1

[11] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), 2. Februar 2000, BGBl. II Nr. 30/2000

[12] Änderung der Signaturverordnung, 30. Dezember 2004, BGBl. II Nr. 527/2004

[13] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008), 7. Jänner 2008, BGBl. II Nr. 3/2008

[14] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBI. I S.876 ff)

[15] Erstes Gesetz zur Änderung des Signaturgesetzes (1.SigÄndG) vom 4. Januar 2005 (BGBl I S. 2 ff)

[16] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.November 2001 (BGBl. I S. 3074ff)

[17] Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002T, 03.04.2002

[18] ETSI SR 002 176 Electronic Signatures and Infrastructure (ESI); Algorithms and Parameters for Secure Electronic Signatures, Version 1.1.1 March 2003

[19] Geeignete Kryptoalgorithmen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. Dezember 2007, Bundesnetzagentur

[20] U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology: FIPS PUB 180-2, Secure Hash Standard, August 2002, including Change Notice 1, February 2004

[21] RSA Laboratories, PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note Version 2.1, Revised June 14, 2002

[22] American National Standards Institute, ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999

[23] DIN V 66291-1, Ausgabe 2000-04 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle

[24] U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology: NIST SP 800-67, Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Version 1, May 2004

[25] American National Standards Institute, ANSI X9.19: Financial Institution Retail Message Authentication, 1986

[26] ISO/IEC 7816-3: 1997 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

[27] ISO/IEC 7816-3: 1997/Amd 1: 2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V

[28] ISO/IEC 7816-4: 2005 Identification cards - Integrated circuit cards – Part 4: Organization, security and commands for interchange

[29] ISO/IEC 7816-8:2004 Identification cards – Integrated circuit cards – Part 8: Commands for security operations

[30] Specification of the generic Secure Signature Application for ACOS EMV-A04, Version 1.1, Austria Card, 2008

[31] Administrator Guidance (AGD_ADM), Version 1.2, Austria Card, 2008

[32] User Guidance (AGD_USR), Version 1.0, Austria Card, 2008

[33] Delivery and Operation Documentation – Delivery, Installation and Generation, Version 1.2, Austria Card, 2008

[34] ACOS EMV-A04 Commands, Version 2.1, Austria Card, 2008

[35] ACOS EMV-A04 Init-Pers-Concept, Version 1.3, Austria Card, 2008