CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9250**
Product / system:	signature creation device ZKA Banking Signature Card, Version 6.32, Type 3
Product manufacturer:	Giesecke & Devrient GmbH Prinzregentenstraße 159 81677 München
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1.0 as of 2005-12-09* Document-number: *20690113_TÜViT_001.01* Author: Stefan Schwingeler
Result:	EAL4 augmented by AVA_MSU.3, AVA_VLA.4
Evaluation stipulations:	one (see chapter 10)
Certifier:	Dr. Christoph Sutter
Certification stipulations:	one (see chapter 11)

Essen, 2005-12-14

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

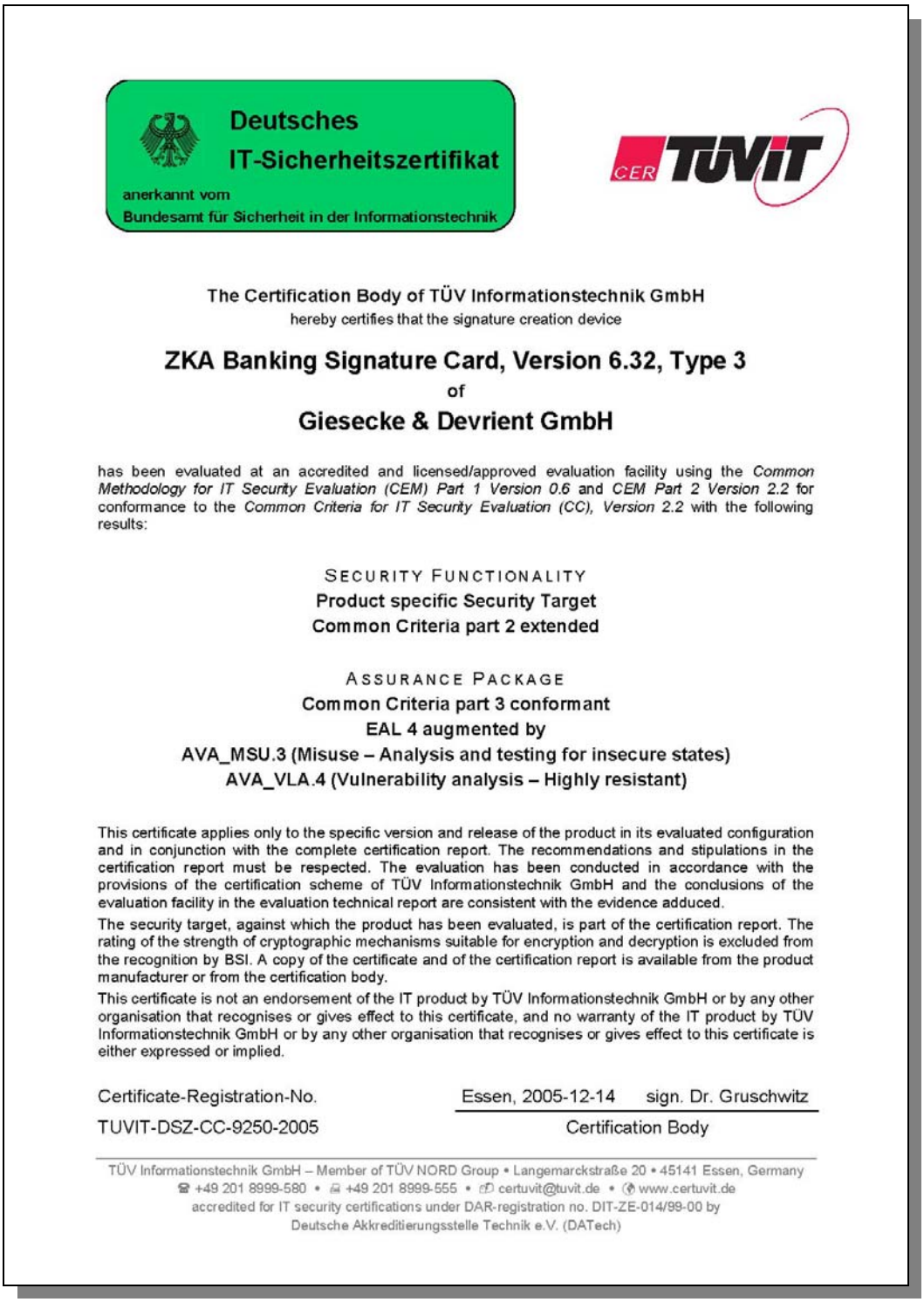
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

CER TÜViT

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the signature creation device

ZKA Banking Signature Card, Version 6.32, Type 3
of
Giesecke & Devrient GmbH

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

SECURITY FUNCTIONALITY
Product specific Security Target
Common Criteria part 2 extended

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 4 augmented by
AVA_MSU.3 (Misuse – Analysis and testing for insecure states)
AVA_VLA.4 (Vulnerability analysis – Highly resistant)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9250-2005

Essen, 2005-12-14 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH – Member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • certuvit@tuvit.de • www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜVIT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – a member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜViT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC - under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The signature creation device ZKA Banking Signature Card, Version 6.32, Type 3 has undergone the certification procedure at TÜViT certification body. It was a re-certification of the ZKA Banking Signature Card, Version 6.31, Type 3 (TUVIT-DSZ-CC-9230-2005 as of 2005-03-11) because of a new completion level (Completion ZKA_1.3 instead of Completion ZKA_1.2) of the ES contained in the initialisation table and a new certificate of the hardware platform (BSI-DSZ-CC-0311-2005 instead of BSI-DSZ-CC-0244-2004) due to an additional production site. (see [BSI 0311])

The evaluation of the signature creation device ZKA Banking Signature Card, Version 6.32, Type 3 was conducted by the evaluation body for IT-security of TÜViT and concluded on December 9, 2005. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is Giesecke & Devrient GmbH. Distributor of the product is Giesecke & Devrient GmbH.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on December 14, 2005. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-18. The product ZKA Banking Signature Card, Version 6.32, Type 3 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the smart card IC with embedded software (ES) ***ZKA Banking Signature Card, Version 6.32, Type 3*** and the EEPROM part "Completion ZKA_1.3" of the ES contained in the initialisation table[3]. The smart card IC, the Philips P5CC036V1C was certified on September 12, 2005 by BSI under certification ID: BSI-DSZ-CC-0311-2005 at the level EAL5 augmented by ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 [BSI 0311]. The evaluation and certification results from the BSI certification have been considered in this certification.

The ES contains the **SECCOS operating system**, which is a multi-application Smart Card OS providing, besides the signature application, ISO 7816 compliant commands for different kinds of banking applications.

The TOE implements a **Secure Signature Creation Device** (SSCD). This includes the generation and secure storage of a SCD/SVD pair and the generation of electronic signatures from 1024 Bit up to a length of 1984 Bit. Digital signature schemes are either PKCS#1 with SHA-1 or ISO/IEC 9796-2 with random numbers with RIPEMD160 (see DIN V 66291-4 or CWA 14890-1:2004).

The TOE is based on the SSCD Type 3 Protection Profile [SSCD T3 PP] and fulfils all essential aspects but it is not compliant to the PP because the trusted channel/path for the transmissions of SVD, DTBS, and VAD is not enforced by the TOE but by the user. The user controls whether the trusted channel/path is established by cryptographic means or by a trusted environment.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 4 (Evaluation Assurance Level 4) augmented by AVA_MSU.3 (Misuse – Analysis and testing for insecure states) and AVA_VLA.4 (Vulnerability analysis - Highly resistant).

1.3 Strength of Functions

The TOE's strength of functions is rated "high" (SOF-high). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

[3] In the following shortly termed ZKA Banking Signature Card.

1.4 Functionality

Except the functional requirement FPT_EMSEC.1 (TOE Emanation) the TOE's security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 extended) [CC]. They can be categorized in the following six categories:

1. cryptographic support,
2. user data protection,
3. identification and authentication,
4. security management,
5. protection of the TSF, and
6. trusted paths/channels.

Chapter 9 lists the security functional requirements in more detail. They are met by eight suitable TOE security functions (TSF):

TSF	Short Description
ACCESS	controls access to data stored in the TOE and to functionality provided by the TOE
ADMIN	manages the administration of the TOE in the initialisation and personalisation phase
AUTH	manages the authentication of the signatory with PINs in the usage phase
SIG	manages the signature creation and SCD/SVD correspondence check functionality in the usage phase
CRYPTO	provides the cryptographic functionality including SHA-1, RIPEMD-160, DES, RSA, check sums, and random number generation
TRUST	manages the establishing of trusted channels/paths
PROTECTION	protects TSF functionality, TSF data, and user data
IC_SF	covers the TSF of the underlying IC platform

A more detailed description of the TOE security functions can be found in section 6.1 of the public ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

All assets, threats, and organisational security policies defined in the ST are taken from the SSCD Type 3 Protection Profile [SSCD T3 PP].

Assets for the TOE comprise the integrity and/or confidentiality of the RSA key pair (SCD/SVD), the data to be signed representation, the verification/reference authentication data, the signature creation function, and the electronic signature.

Any human user or TOE external process acting on his behalf is regarded as an attacker.

The 8 threats deal with loss of confidentiality and integrity of assets as well as identity usurpation.

The 3 organisational security policies contain the requirement that the TOE is a secure signature creation device that is used together with trustworthy applications in the framework of the EU directive 1999/93/EC to create qualified electronic signatures.

A more detailed description of the threats and organisational security policies can be found in sections 3.2 and 3.3 of the public ST, which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered to the card issuer in one fixed configuration. To finalize the TOE, the initialisation table must be loaded during the initialisation phase. The initialisation table contains the EEPROM part “Completion ZKA_1.3” of the ES and the SECCOS file-system, that must fulfil the requirements given in the TOE documentation (see chapter 6). The initialisation tables BSP2G3XEA_1, BSP2G3XEA_3, SDP2G3F0E_2, and SWP2G3H0E_1 were considered in this evaluation and fulfil the requirements.

1.7 Assumptions about the Operating Environment

According to the life-cycle of the TOE, 5 different environments are assumed for the TOE:

1. Design environment: including OS and application design (responsibility: Giesecke & Devrient GmbH) as well as HW design (responsibility: Philips GmbH);
2. Fabrication environment: including the HW fabrication as well as OS and application implementation (responsibility: Philips GmbH);
3. Initialisation environment: corresponding to the start of the operational phase where general application data is loaded (responsibility: card initialising facility, e. g. Giesecke & Devrient GmbH);
4. Personalisation environment: generation of the SCD/SVD RSA key pair and loading of personal application data (responsibility: card personalizing facility, e. g. Giesecke & Devrient GmbH);
5. Usage environment normal usage of the TOE by the end-user, e. g. signature generation.

The life-cycle of the TOE can be found in section 2.2.2 of the public ST, which is attached as part D of this certification report.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by the TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is the ZKA Banking Signature Card Version 6.32, Type 3 with EEPROM part “Completion ZKA_1.3” of the ES contained in the initialisation table.

The TOE delivery to the card issuer consists of the following parts:

1. TOE Documentation (see chapter 6)
2. Hardware part of the TOE:
   - Chip modules with Philips P5CC036V1C (ROM mask of the TOE already implemented)
3. Software part of the TOE:
   - “Completion ZKA_1.3” (contained in signed initialisation tables[4])

Versions of the ROM mask and the initialisation table can be verified as described in chapter 6 of the user guidance.

[4] The initialisation tables BSP2G3XEA_1, BSP2G3XEA_3, SDP2G3F0E_2, and SWP2G3H0E_1 were considered in the evaluation.

3 Security Policy

Within the security target 4 different security policies are defined:

Policy Name	Description
SVD TRANSFER SFP	only the administrator and signatory are allowed to export the public key (SVD)
INITIALISATION SFP	only the administrator and signatory are allowed to generate the SCD/SVD key pair if the TOE is in a respective state
PERSONALISATION SFP	only the administrator is allowed to create reference authentication data
SIGNATURE-CREATION SFP	only the signatory is allowed to create signatures when using an authorised signature creation application and if the TOE is in a respective state

A more detailed description of the different security policies can be found in section 5.1.2.2 of the public ST, which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following two usage assumptions are defined in the ST and must be regarded when using the TOE. They are taken from the SSCD Type 3 Protection Profile [SSCD T3 PP]:

Assumption	Description
A.CGA	Trustworthy certificate-generation application (CGA) 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 (SCA) 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.

4.2 Environmental Assumptions

It is assumed that the TOE is used in the environment described in section 1.7 of this certification report.

4.3 Clarification of Scope

The main focus of this certification is the functionality of the TOE as a secure signature creation device as described in the security target. The functionality of additional commands of the banking applications are not part of this certification. Within the evaluation the evaluator checked that these commands do not violate the TSP.

5 Architectural Information

The TOE comprised two major components: The smart card IC Philips P5CC036V1C and the embedded software (ES). The smart card IC has been certified previously by BSI under certification ID BSI-DSZ-CC-0311-2005. For architectural information on the smart card IC see the corresponding certification report from BSI [BSI 0311]. The embedded software can be divided into 7 subsystems:

Name of Subsystem	Description
Access Control	controls the rights to access the resources of the TOE
Setup	provides procedures to setup resources after start-up of the system including the reset of all security states
Commands	performs the processing of commands sent via the serial interface to the TOE
Application Data and Basic Functions	holds the data needed to drive the operating system and the applications
Crypto Functions	contains functionality for cryptographic support
Secure Messaging	ensures secure communication between TOE and user, and TOE and remote IT products
Hardware	contains the security functions of the hardware

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- Administrator guidance ZKA Banking Signature Card V6.32 Type 3, version 3.6, 2005-11-16,
- User Guidance ZKA Banking Signature Card V6.32 (Type 3), version 1.3, 2005-11-16,
- Generic Signature Application for ZKA Banking Signature Card V6.32 (Type 3) – Security Relevant Sections, version 3.0, 2005-11-16, and
- Installation, generation and start up, ZKA Banking Signature Card V6.32 (Type 3), version 2.1, 2005-11-16.

7 IT Product Testing

The tests performed by the developer were performed on the TOE, on specially modified TOEs and with simulators in the initialisation, personalisation and usage phase.

The developer tested the TOE with the overall objectives to verify that the TOE Security Functions satisfy the requirements as specified in the Functional Specifications (FSP) and in the High Level Design (HLD).

The developer's TOE testing includes about 410 test cases for 8 TOE Security Functions.

The evaluation body repeated the tests of the developer and performed independent penetration testing. The testing confirmed that the TOE is resistant against attacks based on the level of high attack potential, that all the obvious vulnerabilities were considered and that the vulnerabilities identified are non-exploitable in the intended operational environment of the TOE.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL4 augmented by AVA_VLA.4 and AVA_MSU.3 and the class ASE for the Security Target Evaluation) are summarised in the following table:

Assurance classes and components		**Verdict**
Security Target evaluation	**CC Class ASE**	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	**CC Class ACM**	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	**CC Class ADO**	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	**CC Class AGD**	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	**CC Class ALC**	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ATE_TAT.1	PASS
Tests	**CC Class ATE**	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	**CC Class AVA**	PASS
Analysis and testing of insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.1 of the public ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UIT.1	Data exchange integrity
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT	**Security management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles

ID	**Class**/Component
FPT	**Protection of the TSF**
FPT_AMT.1	Abstract machine testing
FPT_EMSEC.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTP	**Trusted path/channels**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Apart from FPT_EMSEC.1 all security functional requirements were taken from [CC] part 2, i. e. the TOE is [CC] part 2 extended

The evaluation performed in accordance to EAL4 augmented by AVA_VLA.4 and AVA_MSU.3 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

TSF *ADMIN*, *AUTH*, *CRYPTO*, and *IC_SF* fulfil the SOF-rating high (SOF-high). The strength of functions rating does not include cryptographic algorithms for encryption and decryption, like DES in TSF CRYPTO. The cryptographic algorithms SHA-1, RIPEMD-160 and RSA with key length between 1024 and 1984 Bit are published in the Bundesanzeiger No. 59 – p. 4695-4696, 2005-03-30 as suitable for the qualified electronic signature and therefore fulfil the requirements for SOF-high.

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to the product "*ZKA Banking Signature Card,Version 6.32, Type 3*". The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluation Stipulations, Comments, and Recommendations

The evaluation technical report contains the following stipulation:

1. The evaluation and subsequent certification are therefore only valid for this version of the TOE. The certification body shall be advised of any modifications made to this configuration and of modifications to the initialisation tables BSP2G3XEA_1, BSP2G3XEA_3, SDP2G3F0E_2, or SWP2G3H0E_1 by the developer. The certification body will then check if the certification results are still valid and initiate further steps concerning a re-evaluation and re-certification, if necessary.

The evaluation technical report contains the following comments and recommendations:

The user and administrator guidance [ADM, USR] makes the following particular constraints for TOE use in order to be resistant to attacks with a high attack potential:

- Authentication processes and secure messaging must use Triple DES algorithm with secret key lengths 128-bit.
- Signature creation keys must be generated with a length of at least 1024-bit.
- PIN code values must have a length of at least 6 and a retry counter of 3.
- PUK code values must have a length of at least 8 and an usage and retry counter of 1. There must be a maximum of 6 different PUK code values.
- It is mandatory to export the public signature key in an authentic way, the exported data shall be linked to a unique ZKA Signature Card
- To verify, that the Initialisation table is a certified variant, the user has to execute the command GET DATA with Parameters P1='DF' P2='20' (see [USR] section 6.2). The website of Giesecke & Devrient GmbH (http://www.gi-de.com) has to provide the necessary information after a search for the term 'SECCOSTABLES'
- If Giesecke & Devrient GmbH will modify the initialisation table, that modified table has to fulfil all requirements of [GEN]. The certification body will then check if the certification results are still valid and initiate further steps.

The delivered guidance [AGD, GEN, USR, IGS] makes the following particular constraints for TOE administration in order to be resistant to attacks with a high attack potential:

- Definition of all files, records and access rules that are relevant with respect to the security of the generic signature application according to the requirements defined in [GEN, ADM].
- Used keys during generation of the personalisation contents should be kept confidential by the personalisation data manager. The transport PIN should be delivered to the user.

- All control data has to be kept secret. The environment has to ensure the secrecy of the control data.
- The ChipPWD must be kept confidential.

The delivered guidance [ADM, USR] makes the following particular constraints for TOE administration in order to be resistant to attacks with a high attack potential:

- The user is responsible to check that the Transport PIN is 5 digit long. He will be responsible to change the Transport PIN and choose a random and secret Signature PIN, which must be at least 6 digit long.
- The signatory shall apply the PUK mechanism only if he is sure that a trusted path is used.
- The signatory makes use of a trustworthy Signature Creation Application SCA only.
- The signatory handles the signature PIN and transport PIN as well as all resetting codes (PUK) in a way that a third party can not get access to this data.
- If present, the Display Message has to be changed regularly in order to prevent attacks. An update is allowed only after a successful device authentication between the application and the card. The signatory shall make sure prior to an update of the Display Message that the device authentication has been performed successfully.

Furthermore an appropriate protection during packaging, finishing, and personalization must be ensured up to delivery to the end-user to prevent any possible copy, modification, retention, theft, or unauthorized use of the TOE and of its manufacturing and test data (the assumption A.Process-Card from the ST [ST_IC_Ph] of the hardware platform).

11 Certification Stipulations and Notes

The stipulation and notes of the evaluation report (see chapter 10) are applicable. There are no additional notes or stipulations resulting from the certification report.

12 Security Target

The public version [ST-lite] of the security target [ST] for *ZKA Banking Signature Card, Version 6.32, Type 3* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CEPS	Common Electronic Purse Specification
CGA	Certificate Generation Application
CM	Configuration Management
CSP	Certification Service Provider
DTBS	Data to Be Signed
EAL	Evaluation Assurance Level
EMV	Europay, Master Card, Visa
EEPROM	Electrical Erasable and Programmable Read Only Memory
ES	Embedded Software
EU	European Union
FSP	Functional Specification
HBCI	Home Banking Computer Interface
HLD	High-level Design
IC	Integrated Circuit
IF	Interface
IGS	Installation, Generation and Start-up
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
RSA	Signature Algorithm of Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SVD	Signature Verification Data
SS	Sub-system
SSCD	Secure Signature Creation Device

SSL	Secure Sockets Layer
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
USR	User Guidance
VAD	Verification Authentication Data
VLA	Vulnerability Analysis

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[ADM] Administrator guidance ZKA Banking Signature Card V6.32 Type 3, version 3.6, 2005-11-16

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI

[BSI 0311] Certification Report – BSI-DSZ-CC-0311-2005 for Philips P5CC036V1C and P5CC009V1C Secure Smart Card Controller from Philips Semiconductors GmbH Business Line Identification, 2005-09-12

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, Version 2.2, January 2004

[ETR] Evaluation Technical Report, TÜV Informationstechnik GmbH,
version 1.0, 2005-12-09, document-number: 20690113_TÜViT_001.01

[GEN] Generic Signature Application for ZKA Banking Signature Card V6.32 (Type 3) – Security Relevant Sections, version 3.0, 2005-11-16

[IGS] Installation, generation and start up, ZKA Banking Signature Card V6.32 (Type 3), version 2.1, 2005-11-16

[SSCD T3 PP]	Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05, EAL4+, 2001-07-05 (certified on 2002-04-03 by BSI under certification ID: BSI-PP-0006-2002) corresponds to CWA 14169:2002, Annex C
[ST]	Security Target ZKA Banking Signature Card, V6.32 (Type 3), Version 1.4, 2005-11-16 confidential document
[ST-lite]	Security Target Lite ZKA Banking Signature Card, V6.32 (Type 3), Version 1.4, 2005-11-16 public version of the Security Target [ST]
[ST_IC_Ph]	Security Target Lite – BSI-DSZ-CC-0244 – Evaluation of the Philips P5CC036V1C Secure Smart Card Controller, Version 1.0, 2004-10-15
[USR]	User Guidance ZKA Banking Signature Card V6.32 (Type 3), version 1.3, 2005-11-16

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

> **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2.
>
> **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

plus one of the following:

> **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3.
>
> **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

> ***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
>
> ***Package name* Augmented** - A PP or TOE is an augmentation of a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

> ***PP Conformant*** - A TOE meets specific PP(s), which are listed as part of the conformance result."

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 1*.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 1: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances.

Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview

„Table 2 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i. e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i. e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_IMT					**1**	**2**	***3***
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance Documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested

"EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL3) - methodically tested and checked

"EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

"EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

"EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL7) - formally verified design and tested

"EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Strength of TOE security functions (AVA_SOF)

AVA_SOF Strength of TOE security functions

"Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large."

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

Application notes

"A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator

should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the public version of the Security Target: "*Security Target Lite ZKA Banking Signature Card, V6.32 (Type 3)*"

Author: Giesecke & Devrient GmbH

Date: 2005-11-16

Version: 1.4

Security Target Lite ZKA Banking Signature Card V6.32 (Type3)

Version 1.4/Status 16.11.2005

F&E

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Contents

1 Introduction

1.1 ST Identification

Title: Security Target for ZKA Banking Signature Card V6.32, Type3

Reference: GDM_STA30_ASE_03

Version Number/Date: Version 1.4/Status 16.11.2005

Origin: Giesecke & Devrient GmbH

TOE: ZKA Banking Signature Card V6.32, Type 3

TOE version: 6.32

TOE documentation:

- Administrator Guidance ZKA banking signature card V6.32 Type 3, V3.6, 16.11.05
- User Guidance ZKA banking signature card V6.32 (Type 3), V1.3, 16.11.05
- Generic Signature Application for ZKA Banking Signature Card V6.32 Type 3 - Security Relevant Sections, V3.0, 16.11.05
- Installation, generation and start-up ZKA Banking Signature Card V6.32 Type 3, V2.1, 16.11.05

HW-Part of TOE: Philips P5CC036V1C

1.2 ST Overview

The aim of this document is to describe the Security Target for the 'ZKA Banking Signature Card V6.32, Type3'.

The related product is the SECCOS Operating System (OS) on a Smart Card Integrated Circuit. It is intended to be used as Secure Signature Creation Device (SSCD) in accordance with the European Directive 1999/93/EC [1], so the TOE consists of the related software in combination with the underlying hardware ('Composite Evaluation'). The functional and assurance requirements for SSCDs defined in Annex III of this EU Directive [1] have been mapped into three Protection Profiles (PPs) for different types of SSCDs (see chap. 2.1.1 for details). The Security Target for the 'ZKA Banking Signature Card V6.32, Type 3' is based on the PP for SSCDs of Type 3 (generation of SCD/SVD pair, storage of Signature Creation Data and Signature Creation Component) [7]. The

only deviation is that the application of Secure Messaging for the communication between the TOE and the SCA is optional and is under control of the cardholder. This deviation from the CWA14169 [7] has been necessary, since TOEs with mandatory use of Secure Messaging can only be used with special terminals supporting Secure Messaging and would be unusable for any other type of terminal.

SECCOS is a fully interoperable ISO 7816 compliant multiapplication Smart Card OS, including a cryptographic library enabling the user to generate high security RSA signatures up to 1984 Bit. The EU compliant Electronic Signature Application is designed for the creation of legally binding Qualified Electronic Signatures as defined in the EU Directive [1]. The various features of SECCOS allow for additional banking applications like EMV application, Geldkarte application, etc..

The software part of the TOE is implemented on the IC Philips SmartMX P5CC036 V1C, which is certified according to CC EAL5+. So the TOE consists of the software part and the underlying hardware. The corresponding Security Target (Lite) [8] is compliant to the BSI-PP-0002-2001 [9].

This document describes

- the Target of Evaluation (TOE)
- the security environment of the TOE
- the security objectives of the TOE and its environment
- and the TOE security functional and assurance requirements.

The assurance level for the TOE is CC **EAL4+**.

The minimum strength level for the TOE security functions is **high** (SOF high).

1.3 CC Conformance

This ST is in accordance with Common Criteria V2.1 (ISO 15408) (see [2], [3], [4]).

This ST is compliant with CC V2.1 Part 2 [3], extended by an additional functional component as stated in [7].

This ST is compliant with CC V2.1 Part 3 [4], level **EAL4** augmented by

- AVA_MSU.3 (Analysis and testing for insecure states)
- AVA_VLA.4 (Highly resistant)

as stated in [7].

The minimum strength level for the TOE security functions is **SOF high**.

1.4 Sections Overview

Section 1 provides the introductory material for the Security Target.

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 [3] and Part 3 [4], that must be satisfied.

Section 6 contains the TOE Summary Specification.

Section 7 provides the compliance claims.

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

Section 9 provides information on applied conventions and used terminology.

Section 10 identifies background material (reference section).

Section 11 provides definitions of frequently used acronyms.

2 TOE Description

2.1 Product Type

2.1.1 Secure Signature Creation Devices

(This description is taken from the SSCD Protection Profile [7] and should be used as general introduction to SSCDs.)

The present document assumes a well defined process signature-creation to take place. The present chapter defines three possible SSCD implementations, referred to as 'SSCD types', as illustrated in Figure 1.

The left part of Figure 1 shows two SSCD components: A SSCD of Type 1 representing the SCD/SVD generation component, and a SSCD of Type 2 representing the SCD storage and signature-creation component. The SCD generated on a SSCD Type 1 shall be exported to a SSCD Type 2 over a trusted channel. The right part of Figure 1 shows a SSCD Type 3 which is analogous to a combination of Type 1 and Type 2, but no transfer of the SCD between two devices is provided.

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

The signatory must be authenticated to create signatures that he sends his authentication data (e.g., a PIN) to the SSCD Type 2 or Type 3 (e.g., a smart card). If the human interface (HI) for such signatory authentication is not provided by the SSCD, a trusted path (e.g., a encrypted channel) between the SSCD and the SCA implementing to HI is to be provided. The data to be signed (DTBS) representation (i.e., the DTBS itself, a hash value of the DTBS, or a pre-hashed value of the DTBS) shall be transferred by the SCA to the SSCD only over a trusted channel. The same shall apply to the signed data object (SDO) returned from a SSCD to the SCA.

SSCD Type 1 is not a personalized component in the sense that it may be used by a specific user only, but the SCD/SVD generation and export shall be initiated by authorized persons only (e.g., system administrator).

SSCD Type 2 and Type 3 are personalized components which means that they can be used for signature creation by one specific user – the signatory -only.

Type 2 and Type 3 are not necessarily to be considered mutually exclusive.

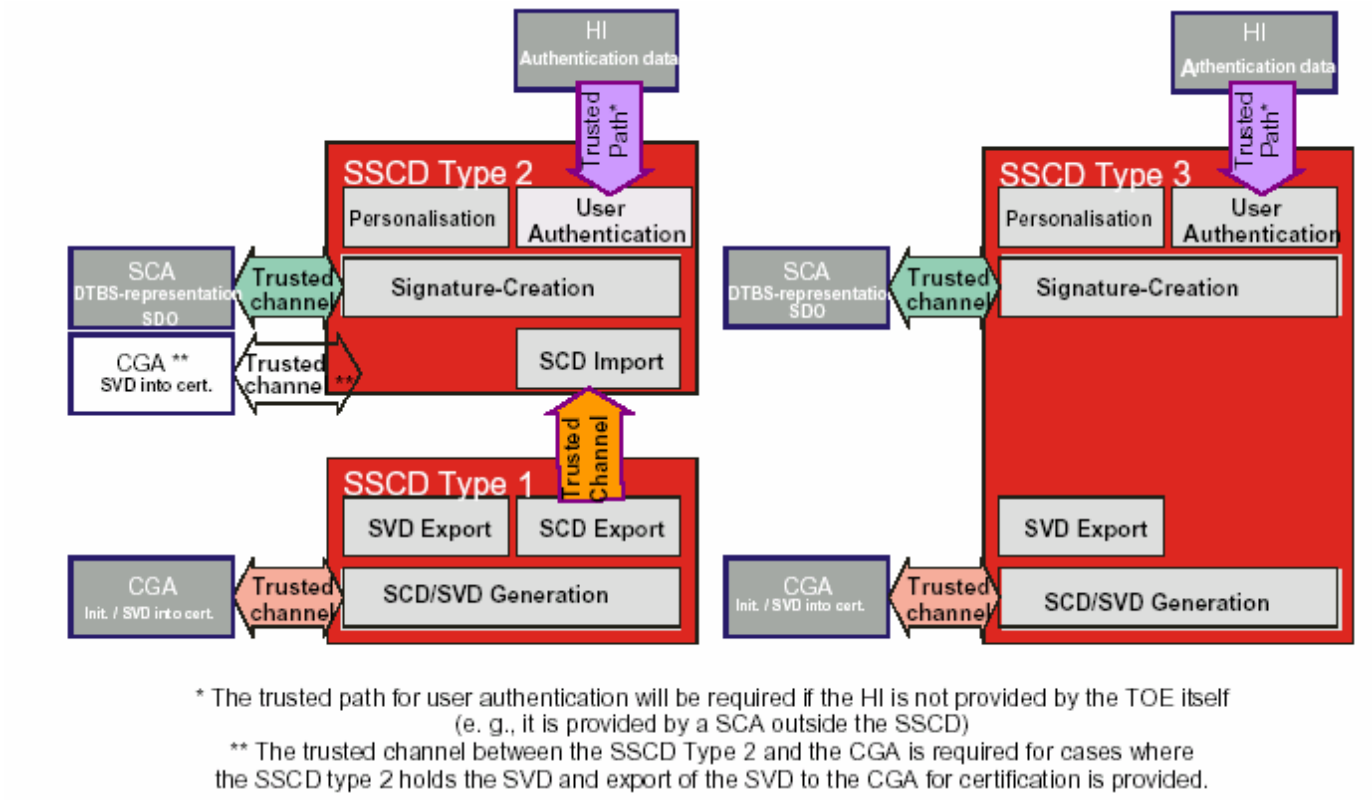


Figure 1: SSCD types and modes of operation

2.1.2 Intended use of the TOE

The TOE is implemented as a Smart Card on an IC and is intended to be used as Secure Signature Creation Device. This includes the Generation and Secure Storage of a SCD/SVD pair and the generation of Qualified Electronic Signatures up to a length of 1984 Bit. The SCD can not be generated in the usage phase.

Beside this the use of multiple separated additional banking applications is possible. Therefore the TOE provides ISO 7816 compliant commands for the different kinds of banking applications. The restriction on the secure generation functionality for keys to prior to the issuance is only applicable to the Signature Application. Any additional application may use the corresponding secure operations in the usage phase. Cryptographic keys of additional applications may be imported, generated, re-imported or re-generated in the usage phase. To ensure for the security of the TOE, the executable code can not be altered in the usage phase.

2.2 Limits of the TOE

2.2.1 Structural view of the TOE

The TOE is a secure signature-creation device (SSCD Type3) according to Directive 1999/93/EC of

the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1]. The destruction of a SCD is mandatory before the TOE replaces it by generating a new pair SCD/SVD. Generation and re-generation of a SCD/SVD pair is possible only before the beginning of the personalisation phase.

The TOE is realised by a smartcard, consisting of the embedded software residing on the underlying hardware (Smart Card integrated circuit, Philips SmartMX P5CC036, certified CC EAL5+). The TOE consists of the operating system SECCOS implemented in the ROM area of the IC, the File System containing the Application for Digital Signatures and other applications installed in the EEPROM of the IC and the underlying IC itself (see Fig. 2). Parts of the operating system may also reside in the EEPROM.

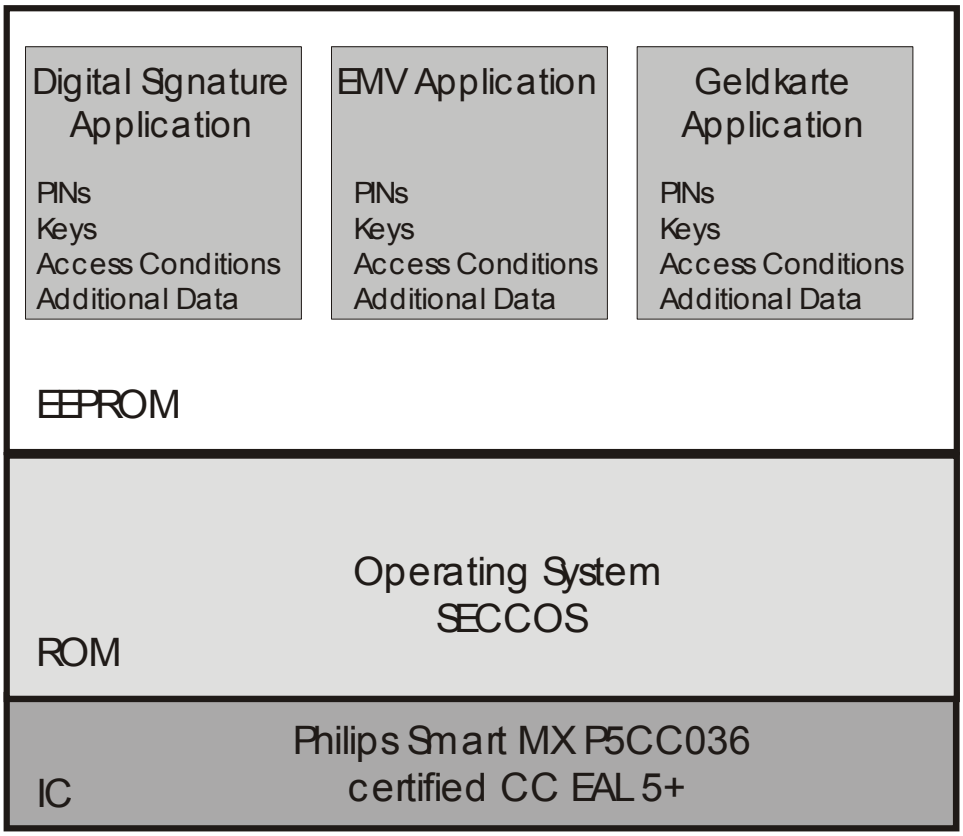


Figure 2: TOE description

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:
(a) after allowing for the data to be signed (DTBS) to be displayed correctly by an appropriate environment
(b) using appropriate hash functions that are, according to [6], agreed as suitable for qualified electronic signatures
(c) after appropriate authentication of the signatory by the TOE
(d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [6].

The TOE ensures for the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The user authenticates himself with the Verification Authentication Data (VAD) against the Reference Authentication Data (RAD) securely stored inside the card. The TOE implements IT measures to support a trusted path to a trusted human interface device that can optionally be connected via a trusted channel with the TOE.

The TOE does not implement the signature-creation application (SCA), that presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. So this ST assumes the SCA as environment of the TOE.

The TOE protects the SCD during the whole life cycle as to be solely used in the signature creation process by the legitimate signatory. The SSCD of Type 3 generates the signatory's SCD and stores it in a secure manner. The TOE will be personalised for the signatory's use by
(1) generation of the SCD
(2) personalisation for the signatory by means of the signatory’s verification authentication data (VAD).
The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP).

From the structural perspective, the SSCD comprises the underlying IC, the SECCOS operating system (OS), the SVD export, SCD storage and use, and signature-creation functionality. The SCA and the CGA (beside optional other applications) are part of the immediate environment of the TOE. They may communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively. In case a trusted channel or trusted path is not established with cryptographic means the TOE shall only be used within a Trusted Environment.

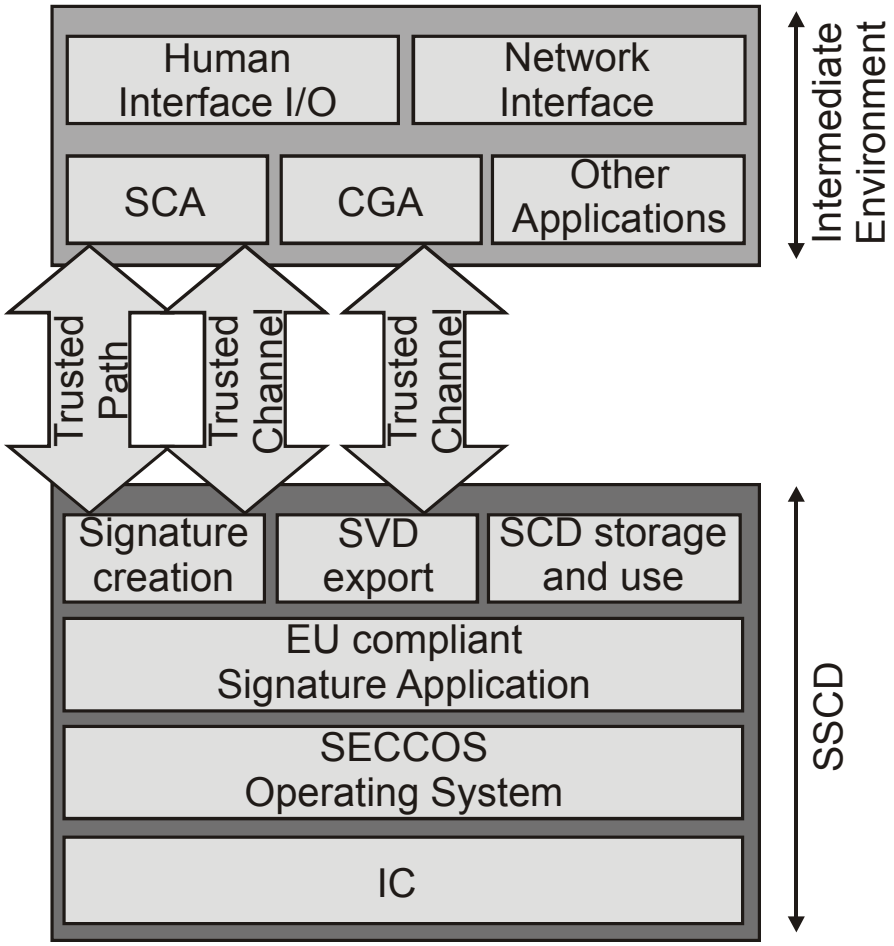


Figure 3: Scope of the SSCD, structural view

Beside the EU compliant Signature Application there are also additional banking applications possible to reside on the TOE like EMV application, Geldkarte application, etc. These applications are using the same underlying IC and OS as the EU compliant Signature Application, but are completely separated from it. So the use of additional applications doesn't influence the security of the Signature Application and have to be regarded as data structures. The TOE has to be defined as the combination of the Signature Application and optional additional applications as shown in Figure 2.

2.2.2 Card Life Cycle

The TOE life cycle is shown in Figure 4. Basically, it consists of a development phase and the operational phase. The development phase includes OS Design and Application Design (responsibility: G&D), HW design (responsibility: Philips), HW Fabrication as well as OS and Application Implementation (responsibility: Philips). The operational phase starts with the initialisation (responsibility: Initialiser: G&D or other card initialising facility), where the general application data is loaded, followed by the personalisation (responsibility: Personaliser : G&D or other card personalising facility) including SCD generation and loading of personal application data. Generation of SCD is performed after loading of initialisation table and prior to loading of personal application data. These phases represent installation, generation, and startup in the CC terminology.

The operational phase is concluded by the usage phase (responsibility for delievery to end user: Card Issuer: Banks). The main functionality in the usage phase is signature-creation including all supporting functionality (e.g. SCD storage and SCD use).

The evaluation process is limited to the development phase including all delivery procedures therein. Since the generation of the TOE is not completed after the development phase, all of the remaining processes have to be in agreement with the IT security requirements defined in chapter 5.

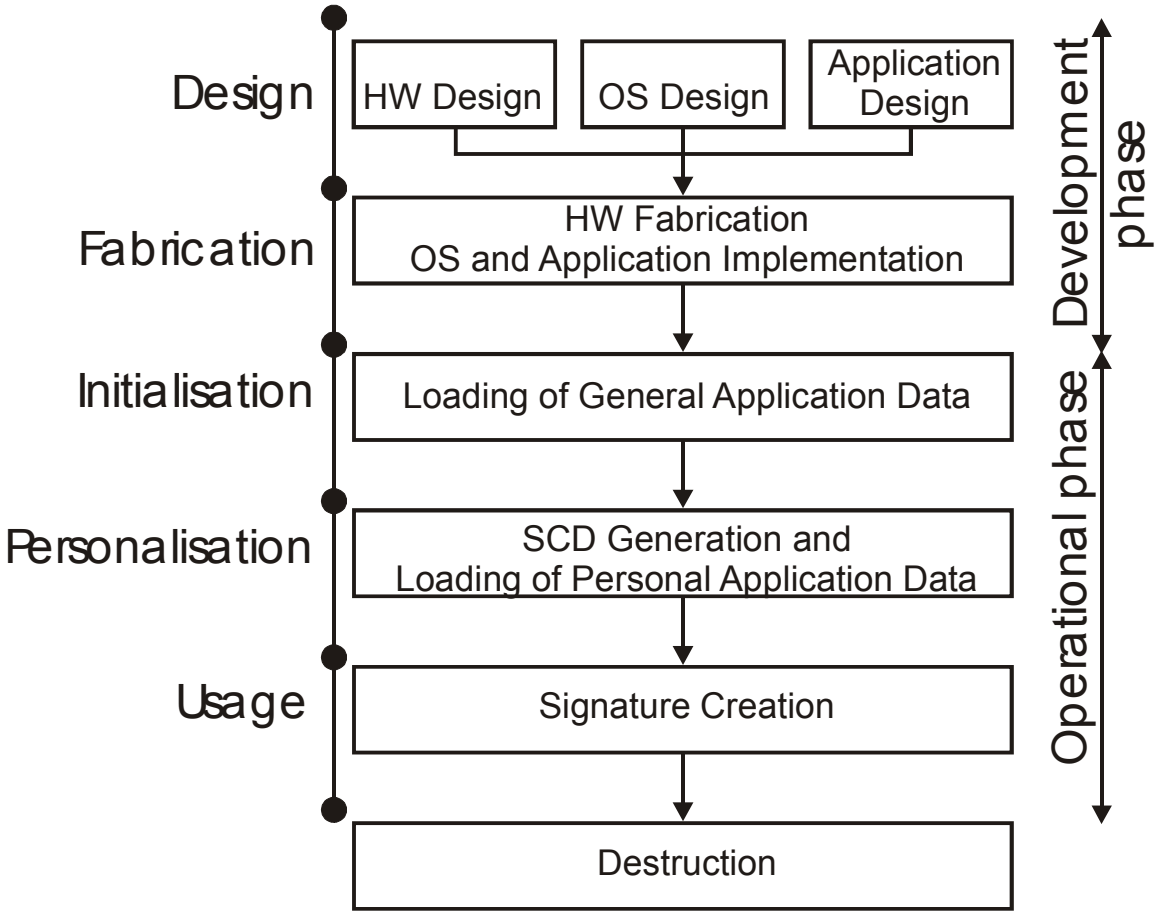


Figure 4. SSCD life cycle

2.2.3 Generation of ROM-Mask and EEPROM Image

As shown in Fig. 2, the Software part of the TOE consists of the SECCOS operating system located in the ROM of the IC and the File System located in the EEPROM. Parts of the operating system may also reside in the EEPROM. The Mask developer (Card manufacturer) (i.e. G&D) creates the ROM mask and sends it to the Chip Manufacturer (see Fig. 5). The Verlage der Kreditwirtschaft send data to the Card manufacturer to be integrated into the Initialisation Image (of the EEPROM) in order to ensure for the authenticity of the Initialisation Image. The Card manufacturer integrates this data into the Initialisation Image created by the Card manufacturer himself and sends the secured Image to the Verlage der Kreditwirtschaft.

The Chip manufacturer generates data to ensure for the authenticity of the Chip that contains the ROM specified in the ROM-Mask. The Chip manufacturer incorporates this data in a special area of the EEPROM of the Chip and delivers this data to the Verlage der Kreditwirtschaft. The Chip manufacturer delivers the secured modules to the Initialiser/Personaliser.

The Verlage der Kreditwirtschaft integrate the data that ensures for the authenticity of the Chip into the Initialisation Image and secures the Initialisation Image by a signature to enable verification of its integrity. The Verlage der Kreditwirtschaft send the Initialisation Image to the Card Initialising Facility (Initialiser) including the data to verify the authenticity and integrity of the Chip and the Initialisation Image. In addition the Verlage send the corresponding Personalisation Data to the Card Personalising Facility (Personaliser). The Card Initialising Facility performs the Initialisation and the Card Personalising Facility performs the Personalisation on the Chips delivered by the Chip manufacturer.

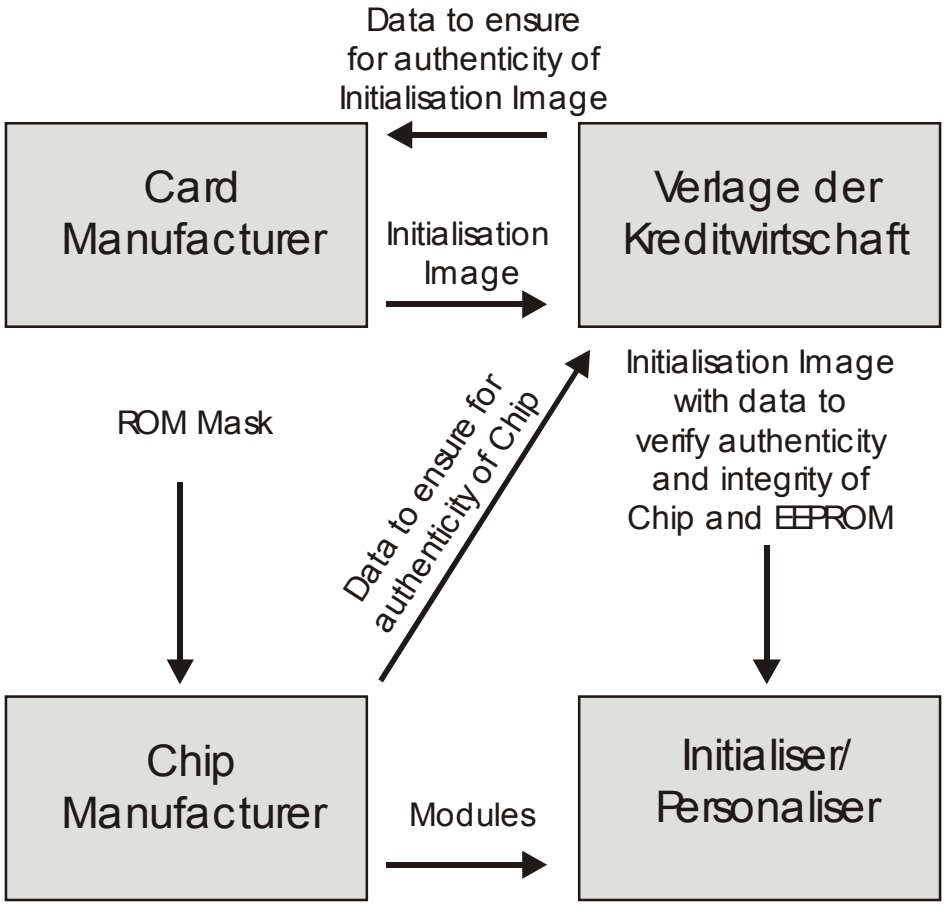


Figure 5: ROM Mask and Initialisation Image generation and delivery

2.3 TOE operational environment

The TOE is used in two different types of operational environment. Prior to the issuance, the TOE has to be completed in the initialsation phase and the personalisation phase. Here the SCD is generated inside the TOE (see Figure 1). After the issuance, the Card Holder controls the TOE. The Card Holder mainly interacts with the TOE via the SCA. The secure communication between the SCA and the TOE is realised by a Trusted Channel (see Figure 1). The Trusted channel can either be realised by using an environment which is trusted by the Card Holder or by using cryptographic means to protect the communication between SCA and SSCD.

According to Figure 1, the SVD has to be exported into the CGA via a Trusted Channel.

2.4 Application Note: Scope of ST application

This ST is intended to be used for CC evaluation of a Secure Signature Creation Device (SSCD) in agreement with the requirements specified in Annex III of [1] as well as the requirements from German signature Act (§17 Abs.1 and 3 Nr.1 [17] and §15 Abs. 1, 4 [18]). Supported cryptographic algorithms are RSA with keylengths from 1024 Bit to 1984 Bit for signature generation and SHA-1

as well as RipeMD160 for Hashing - all of them in agreement with [6]. Beside the signature application itself there are additional applications possible, which reside also on the SSCD and are completely separated from the signature application. While the main application scenario of a SSCD will assume a qualified certificate (i.e. an electronic attestation of the SVD corresponding to the signatory's SCD) to be used in combination with a SSCD, there still is a large benefit in the security when such a SSCD is applied in other areas, since other applications can use the trustworthy evaluated security related functionality used by the signature application.

According to [1], for the generation of a legally binding advanced electronic signature based on a qualified certificate the use of a SSCD as well as the existence of a qualified certificate for the signatory's SVD is mandatory. In addition, the EU Directive [1] does not prevent the use of a SSCD together with a non-qualified certificate and still regard the device itself as SSCD.

3 TOE Security Environment

This chapter has been taken from [7] without modification, except for Note1 for the Assets defined in this chapter.

Assets:

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

2. SVD: public key linked to the SCD and used to perform an electronic signature verification(integrity of the SVD when it is exported must be maintained).

3. DTBS and DTBS-representation: set of data, or its representation which is intended to be signed (Their integrity must be maintained).

4. VAD: PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD must be maintained)

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

6. Signature-creation function of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures)

7. Electronic signature: (Unforgeabilty of electronic signatures must be assured).

Note1: Biometric authentication is not supported by the TOE. Therefore 'biometric data' or 'biometric authentication references' are not used by the TOE.

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.

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 to Security

T.Hack_Phys *Physical attacks through the TOE interfaces*

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

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

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

T.SCD_Derive *Derive the signature-creation data*

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

T.Sig_Forgery *Forgery of the electronic signature*

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

T.Sig_Repud *Repudiation of signatures*

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

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

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

T.DTBS_Forgery *Forgery of the DTBS-representation*

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory 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 1) and is created by a SSCD.

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

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

4 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions. This chapter has been taken from [7] without modification. except for adding **OE.SCA_Trusted_Environment** in chap. 4.2 and adapting **OT.DTBS_Integrity_TOE** (chap.4.1) and **OE.HI_VAD** (chap. 4.2).

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 the 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*

In case the Trusted Path or Trusted Channel is established by cryptographic means the TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBSrepresentation 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 alia
(a) the name of the signatory controlling the TOE,
(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,
(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA *CGA verifies the authenticity of the SVD*

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

OE.HI_VAD *Protection of the VAD*

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

OE.SCA_Data_Intend *Data intended to be signed*

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

OE.SCA_Trusted_Environment *Trusted environment of SCA*

In case the Trusted Path or Trusted Channel is not established by cryptographic means the environment of the TOE protects (i) the confidentiality and integrity of the VAD entered by the user via the SCA human interface provided and sent to the TOE and (ii) the integrity of the DTBS sent by the SCA to the TOE.

(OE.SCA_Trusted_Environment is not part of the SSCD PP [7].)

5 IT Security Requirements

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

Security functional requirements components given in section 5.1 “TOE security functional requirements” excepting FPT_EMSEC.1 which is explicitly stated, are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3]. Operations for assignment, selection and refinement have been made.

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

Any operations performed in the E-Sign F PP [7] are identified by an underline.
Any uncompleted operations from the E-Sign F PP [7] that have been completed in this ST are identified by an underline and in *italic*. Beside these operations the following chapters have been taken from [7] without modification except for chapter 5.1.4.6 (FMT_SMF.1), which is not part of [7] but had to be introduced due to [16].
Any changes to operations performed in the E-Sign F PP [7] and application notes defined in [7] are marked by segmented unterline. Any other changes are marked in the text.

5.1 TOE Security Functional Requirements

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *G&D RSAGen* and specified cryptographic key sizes *between 1024 bit and 1984 bit* that meet the following: *[6]*.

5.1.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1/ RE-GENERATION	The TSF shall destroy cryptographic keys in case of regeneration of a new SCD in accordance with a specified cryptographic key destruction method *physical deletion of key value* 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.

5.1.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/ CORRESP	The TSF shall perform SCD / SVD correspondence verification in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *between 1024 bit and 1984 bit* that meet the following: *[6]*.
FCS_COP.1.1/ SIGNING	The TSF shall perform digital signature-generation in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *between 1024 bit and 1984 bit* that meet the following: *[6]*.

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	The TSF shall enforce the Signature-creation SFP on 1. sending of DTBS-representation by SCA, 2. signing of DTBS-representation by Signatory.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are

User, subject or object the attribute is associated with	Attribute	Status
General attribute		
User	Role	Administrator, Signatory
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

FDP_ACF.1.1/ Signature-creation SFP	The TSF shall enforce the Signature-creation SFP to objects based on General attribute and Signature-creation attribute group.
FDP_ACF.1.2/ Signature-creation SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with the security attribute “role” set to “Signatory” is allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”.
FDP_ACF.1.3/ Signature-creation SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature-creation SFP	The TSF shall explicitly deny access of subjects to objects based on the rule: (a) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS which is not sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “yes”. (b) User with the security attribute “role” set to “Signatory” is not allowed to create electronic signatures for DTBS sent by an authorised SCA with SCD by the Signatory which security attribute “SCD operational” is set to “no”.

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature. The Signatory controls wether the trusted channel required by FTP_ITC.1.3/SCA DTBS is established by cryptographic means or by a trusted environment.

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

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

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

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

Application note:

A SCA is authorised to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature. The Signatory controls wether the trusted channel required by FTP_ITC.1.3/SCA DTBS is established by cryptographic means or by a trusted environment.

5.1.2.5 Subset residual information protection (FDP_RIP.1)

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

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

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

1. SCD

2. RAD

3. SVD (if persistent stored by TOE).

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

integrity checked persistent 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)

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

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

FDP_UIT.1.1/ TOE DTBS — The TSF shall enforce the Signature-creation SFP to be able to receive the DTBS-representation in a manner protected from modification, deletion and insertion errors.

FDP_UIT.1.2/ TOE DTBS — The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

Application note:

Protection for FDP_UIT.1.1/SVD Transfer and FDP_UIT1.1/TOE DTBS can either be assured by cryptographic means or by use of a Trusted Environment.

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 *3* unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

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

5.1.3.2 User attribute definition (FIA_ATD.1)

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

5.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [

1. Identification of the user by means of TSF required by FIA_UID.1.
2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.]

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

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

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

5.1.3.4 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

1. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
2. Establishing a trusted channel between the SCA and the TOE

by means of TSF required by FTP_ITC.1/DTBS import.]

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

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to enable the 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 to restrict the ability to modify the security attributes SCD operational to Signatory.

5.1.4.3 Secure security attributes (FMT_MSA.2)

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

5.1.4.4 Static attribute initialisation (FMT_MSA.3)

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

Refinement
The security attribute of the SCD “SCD operational” is set to “no” after generation 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 the RAD to Signatory.

5.1.4.6 Specification of Management (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *security function management, security attribute management and TSF data management.*

Note: This chaper was not part of [7] but had to be introduced due to [16].

5.1.4.7 Security roles (FMT_SMR.1)

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

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, at the condition Reset of the TOE and SCD generation* 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 about IC power consumption and command execution time* in excess of *non useful information* enabling access to RAD and SCD.

FPT_EMSEC.1.2 The TSF shall ensure *S.OFFCARD* are unable to use the following interface *contacts VCC, GND, IO* to gain access to RAD and SCD.

Application note:

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

internal states, electromagnetic radiation due to internal operation, radio emission.

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

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

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *inconsistencies in the calculation of the signature.*

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 *tampering of the physical operating conditions voltage supply, clock frequency and temperature beyond the valid limits* to the *IC* 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, periodically during normal operation, at the condition Reset of the TOE* to demonstrate the correct operation of the TSF.

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

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

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Inter-TSF trusted channel (FTP_ITC.1)

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

Application Note:

A Trusted Channel can either be established by cryptographic means or assured by a Trusted Environment. In the latter case the TOE identifies the establishment of a Trusted Channel by successful user authentication.

5.1.6.2 Trusted path (FTP_TRP.1)

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

FTP_TRP.1.1/ TOE	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ TOE	The TSF shall permit *local users* to initiate communication via the trusted path.
FTP_TRP.1.3/	The TSF shall require the use of the trusted path for *none*.

TOE

Application Note:

A Trusted Path can either be established by cryptographic means or assured by a Trusted Environment. In the latter case the TOE identifies the establishment of a Trusted Path by successful user authentication.

5.2 TOE Security Assurance Requirements

Table 5.1 : Assurance Requirements: EAL(4)

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

5.2.1 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.
ACM_CAP.4.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.4.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.8C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.9C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.10C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.4.11C	The CM system shall support the generation of the TOE.
ACM_CAP.4.12C	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)

ACM_SCP.2.1D The developer shall provide CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

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)

ADO_IGS.1.1C The documentation shall describe 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 modeled.

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 securityrelevant 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 welldefined.
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 implementationdependent 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)

AVA_VLA.4.1D	The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.
AVA_VLA.4.2D	The developer shall document the disposition of identified vulnerabilities.
AVA_VLA.4.1C	The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.4.2C	The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
AVA_VLA.4.3C	The evidence shall show that the search for vulnerabilities is systematic.
AVA_VLA.4.4C	The 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: *none*.

5.3.1.2 Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1/ CGA	The TSF shall perform import the SVD in accordance with a specified cryptographic key access method import through a secure channel that meets the following: *none*.

5.3.1.3 Data exchange integrity (FDP_UIT.1)

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

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

5.3.1.4 Inter-TSF trusted channel (FTP_ITC.1)

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

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 or RIPEMD-160* and cryptographic key sizes none that meet the following: *[6].*

5.3.2.2 Data exchange integrity (FDP_UIT.1)

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

5.3.2.3 Inter-TSF trusted channel (FTP_ITC.1)

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

SCA DTBS	channel for signing DTBS-representation by means of the SSCD.

5.3.2.4 Trusted path (FTP_TRP.1)

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

FTP_TRP.1.1/ SCA	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ SCA	The TSF shall permit *local users* to initiate communication via the trusted path.
FTP_TRP.1.3/ SCA	The TSF shall require the use of the trusted path for *none.*

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 [1], ANNEX II “Requirements for certification-service-providers issuing qualified certificates”, literal (d). The CSP shall verify that this person holds the SSCD which implements the SCD corresponding to the SVD to be included in the qualified certificate.

R.TRP_Environment *Trusted environment for the TOE and local user*

In case the Trusted Path or Trusted Channel is not established by cryptographic means the environment, in which the TOE is used, shall keep confidentiality and integrity of the VAD and integrity of the DTBS.

(**R.TRP_Environment** is not part of the SSCD PP [7].)

6 TOE Summary Specification

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

6.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

In the following table all TOE Security Functions are listed and if appropriate a SOF claim is stated. The assessment of cryptographic algorithms is not part of this CC evaluation.

Table 6.1 : SOF claims for TOE Security Functions

TOE Security Function	SOF claim	Description
SF.ACCESS	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.ADMIN	high	There is a probabilistic password mechanism for the authentication of the administrator.
SF.AUTH	high	There is a probabilistic password mechanism for the authentication of the signatory.
SF.SIG	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.CRYPTO	high	The random number generators and hash functions are probabilistic mechanisms. The deterministic random number generator is rated K3 (high) according to AIS20 [14].
SF.TRUST	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.PROTECTION	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.IC_SF	high	Several Security Functions of the IC are realised by probabilistic or permutational noncryptographic mechanisms. For the rating of the HW-RNG according to AIS31 [13] see [15].

The SFs described in 6.1.1 to 6.1.7 are realised by software components supported by the underlying hardware in accordance with the description in 6.1.8 (hardware related SF).

6.1.1 SF.ACCESS Access Control

Before the TSF performs an operation requested by a user, this Security function checks if the operation specific requirements on user authorisation and protection of communication data are fulfilled.

This Security Function is composed of:

1) Maintenance of the Security Attributes “Role”, “SCD/SVD management”, “SCD operational”, “RAD” and “sent by an authorised SCA”.
2) The generation of the SCD/SVD pair is for the Administrator allowed only if “SCD/SVD management” is set to "authorised".
3) The export of the SVD is allowed for the Administrator and the Signatory. The usage of a trusted channel for the export of the SVD is required.
4) The creation of RAD is allowed for the administrator during the personalisation phase.
5) The creation of a signature is only for the Signatory allowed during the usage phase if the DTBS is sent by an authorised SCA and “SCD operational” is set to “yes”.
6) Establishing a trusted path or a trusted channel is allowed before Identification and Authentication of the user. Other TSF mediated actions on behalf of a user require his prior successful authentication.
7) Enabling the signature-creation function is only allowed for the Signatory.
8) Modifying RAD and “SCD operational” is only allowed for the Signatory.
9) Modifying “SCD/SVD management” is only allowed for the Administrator.

6.1.2 SF.ADMIN Administration of the TOE

The administration of the TOE is managed by this Security Function. The TOE administration is mainly done in the initialisation and personalisation phase.

This Security Function is composed of:

1) Authentication mechanism for the Administrator.
2) Secure Modification of the Security Attributes “Role” and “SCD/SVD management”.
3) Management of SCD/SVD generation with key sizes between 1024 bit and 1984 bit.
4) Before a new SCD is generated the old SCD is physically deleted.
5) The security attribute “SCD operational” is set to “no” after generation of the SCD. The Administrator is allowed to specify an alternative value.
6) The SVD is exported without associated security attributes.
7) Creation of RAD during the personalisation phase.

This Security Function has the level of strength SOF-high.

6.1.3 SF.AUTH Authentication of the Signatory

The authentication of the Signatory is managed by this Security Function. This Security function is only active during the usage phase.

This Security Function is composed of:

1) Authentication mechanism for the Signatory. If there are more than 3 consecutive failed authentication attempts the RAD is blocked.
2) Secure Modification of the Security Attributes “Role”, “SCD operational” and “RAD”.
3) Enabling the signature-creation function.

This Security Function has the level of strength SOF-high.

6.1.4 SF.SIG Signature Creation

The Signature Creation is managed by this Security Function. This Security function is only active during the usage phase.

This Security Function is composed of:

1) Receiving hash values (without associated security attributes) and calculating hash values for the signing process,
2) Ensuring the integrity of the hash value used for the signing process,
3) Generating digital signatures according to DIN V66291-4[11] and PKCS#1[12], both schemes are described in DIN V66291-4[11]:
   - chapter 2.1.1. of DIN V66291-4[11] specifies “DSI according to ISO/IEC 9796-2 with Random Number”, for this scheme the hash algorithm RIPEMD 160 is used,
   - chapter 2.1.2. of DIN V66291-4[11] specifies “DSI according to PKCS#1”, for this scheme the hash algorithm SHA-1 is used,

   The hash calculation and the RSA calculation is provided by SF.CRYPTO.
4) Proving the correspondence of SCD and SVD.

6.1.5 SF.CRYPTO Cryptographic Support

This Security Function provides the cryptographic support for the other Security Functions.

This Security Function is composed of:

1) Calculating hash values according to SHA-1 and RIPEMD-160,
2) RSA calculation with key sizes between 1024 bit and 1984 bit,
3) DES calculation with key sizes of 112 bit,
4) Random number generation, e.g. used for key generation and authentication process,
5) Calculation of block check values to insure data integrity.

6) Generation of RSA key pairs with key sizes between 1024 bit and 1984 bit.

This Security Function has the level of strength SOF-high.

6.1.6 SF.TRUST Trusted Communication

This Security Function manages the establishing of trusted channels/paths and the application of the protection of the communication data.

This Security Function is composed of:

1) Establishing a trusted channel/path based on mutual authentication with negotiation of a symmetric cryptographic key used for the protection of the communication data. The mutual authentication is based on a random challenge and a corresponding response.
2) Ensuring the confidentiality of communication data, e.g. by encrypting the communication data using symmetric cryptography. This is for example used to confidentially import the VAD.
3) Ensuring the integrity of communication data, e.g. by calculating a cryptographic checksum for the communication data using symmetric cryptography.
4) Secure Modification of the Security Attributes “sent by an authorised SCA”.

This Security Function has the level of strength SOF-high.

6.1.7 SF.PROTECTION Protection of TSC

This Security Function protects the TSF functionality, TSF data and user data.

This Security Function is composed of:

1) Upon the de-allocation of resources from SCD, VAD and RAD the information content of these resources is physically deleted.
2) Ensuring the integrity of SCD, SVD and RAD when using them.
3) Demonstrating the correct operation of the IC.
4) Demonstrating the correct operation of the TSF.
5) Hiding information about IC power consumption and command execution time, to ensure that the IC contacts VCC, GND and IO can not be used to gain access to RAD and SCD.
6) Preserving a secure state in the case of inconsistencies in the calculation of the signature.

6.1.8 SF.IC_SF Security Functions of the IC

This Security Function covers the Security Functions of the IC [8].

This Security Function is composed of:

1) Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.
2) Resistance to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.
3) Random number generation.
4) Cryptographic support for DES calculations, RSA calculations and RSA key pair generation.

6.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 5.2.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

Table 6.1 : References of Assurance Measures

Assurance Measures	Description
AM_ACM	The configuration management is described in GDM_STA30_ACM_00.
AM_ADO	The delivery, installation, generation and start-up of the TOE is described in GDM_STA30_ADO_00.
AM_ADV	The representing of the TSF is described in GDM_STA30_ADV_SPM_00 for security policy modelling, in GDM_STA30_ADV_FSP_00 for functional specification, in GDM_STA30_ADV_HLD_00 for high level design, in GDM_STA30_ADV_LLD_00 for low level design, in GDM_STA30_ADV_IMP_00 for implementation representation and in GDM_STA30_ADV_RCR_00 for representation correspondence.
AM_AGD	The guidance documentation is described in GDM_STA30_AGD_USR_00 for the user and in GDM_STA30_AGD_ADM_00 for the administrator.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in GDM_STA30_ALC_00
AM_ATE	The testing of the TOE is described in GDM_STA30_ATE_00.
AM_AVA	The vulnerability assessment for the TOE is described in GDM_STA30_AVA_MSU_00 for the misuse, in GDM_STA30_AVA_SOF_00 for the strength of TOE security functions and in GDM_STA30_AVA_VLA_00 for the vulnerability

	analysis.

Note: Reference endnumbers may change during evaluation process (e.g. GDM_STA30_AVA_VLA_00 may become GDM_STA30_AVA_VLA_02).

7 PP Claims

7.1 PP Reference

The Security Target for the 'ZKA Banking Signature Card V6.32, Type 3' is based on the PP for SSCDs of Type 3 (generation of SCD/SVD pair, storage of Signature Creation Data and Signature Creation Component) [7]. The only deviation is that the application of Secure Messaging for the communication between the TOE and the SCA is optional and is under control of the cardholder.

7.2 PP changes and additions

The followong changes and additions with respect to the SSCD PP [7] have been made:

- OT.DTBS_Integrity_TOE (changed)
- OE.HI_VAD (changed)
- OE.SCA_Trusted_Environment (added)
- FDP_ITC.1.3/ DTBS (change of Application Note)
- FMT_SMF.1 (added)
- FTP_ITC Application Note (added)
- FTP_TRP.1.3/TOE (changed)
- FTP_TRP.1.3/SCA (changed)
- R.TRP_Environment (added)

8 Rationale

The chapters 8.1 to 8.6 as well as 8.8 and 8.9 have been taken from [7] with modifications only according to the changes in the previous chapters.

8.1 Introduction

The tables in sub-sections 8.2.1 “Security Objectives Coverage” and 8.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE .

8.2 Security Objectives Rationale

8.2.1 Security Objectives Coverage

Table 8.1: Security Environment to Security Objectives Mapping

Threads - 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	OE.SCA_Trusted_Environment
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	X
T.SigF_Misuse										X	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	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						

8.2.2 Security Objectives Sufficiency

8.2.2.1 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 [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by OE.CGA_QCert. OE.SCA_Data_Intend provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. OT.Sig_Secure and OT.Sigy_SigF address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device) establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by OT.Sigy_SigF ensuring that the SCD is under sole control of the signatory and OT.SCD_Unique 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.

8.2.2.2 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 [1], 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 than does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign.

The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by verifying the integrity of the DTBS-representation. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.SCA_Data_Indent and OE.SCA_Trusted_Environment.

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 [1], 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), OE.SCA_Trusted_Environment (Trusted environment of the SCA), 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, OE.SCA_Trusted_Environment 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 signaturecreation 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) , OE.SCA_Trusted_Environment (Trusted environment of the SCA) 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, OE.SCA_Trusted_Environment 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.

8.2.2.3 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.

8.3 Security Requirements Rationale

8.3.1 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				X	X				X			
FCS_CKM.4		X		X								
FCS_COP.1/CORRESP					X							
FCS_COP.1/SIGNING												X
FDP_ACC.1/SVD_TRANSFER SFP						X						
FDP_ACC.1/INITIALISATION SFP			X	X								
FDP_ACC.1/PERSONALISATION SFP											X	
FDP_ACC.1/SIGNATURE-CREATION SFP										X	X	
FDP_ACF.1/INITIALISATION SFP			X	X								
FDP_ACF.1/SVD_TRANSFER SFP						X						
FDP_ACF.1/PERSONALISATION SFP											X	
FDP_ACF.1/SIGNATURE-CREATION SFP										X	X	
FDP_ETC.1/SVD TRANSFER						X						
FDP_ITC.1/DTBS										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	
FMT_SMR.1				X							X	
FPT_AMT.1		X		X								X
FPT_EMSEC.1	X											
FPT_FLS.1				X								
FPT_PHP.1							X					

FPT_PHP.3								X				
FPT_TST.1		X										X
FTP_ITC.1/SVD TRANSFER						X						
FTP_ITC.1/DTBS IMPORT										X		
FTP_TRP.1/TOE											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	OE.SCA_Trusted_Environment
FCS_CKM.2/CGA	X				
FCS_CKM.3/CGA	X				
FCS_COP.1/SCA HASH			X		
FDP_UIT.1/SVD IMPORT				X	
FTP_ITC.1/SVD IMPORT				X	
FDP_UIT.1/SCA DTBS			X		
FTP_ITC.1/SCA DTBS			X		
FTP_TRP.1/SCA		X			
R.Sigy_Name	X				
R.TRP_Environment		X			X

Table 8.4 : Assurance 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

8.3.2 Security Requirements Sufficiency

8.3.2.1 TOE Security Requirements Sufficiency

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

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

OT.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 corresponding to the actual TOE (i.e., FMT_MSA.1/ADMINISTRATOR, FMT_MSA.3), and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

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

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_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 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by FCS_COP.1/CORRESP

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

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

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

The security functions specified by FDP_ACC.1/PERSONALISATION SFP, FDP_ACC.1/SIGNATURE-CREATION SFP, FDP_ACF.1/PERSONALISATION SFP, FDP_ACF.1/SIGNATURE-CREATION SFP, FMT_SMF.1, 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_SMF.1, FMT_MSA.2, and FMT_MSA.3 ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as FMT_MSA.1/SIGNATORY provides that the control of corresponding security attributes is under signatory's control.

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

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

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

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1/SIGNING which ensures the cryptographic robustness of the signature algorithms. The security functions specified by FPT_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 and FDP_ETC.1/SVD TRANSFER ensure that only authorised user can export the SVD to the CGA.

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

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

8.3.2.2 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 or the Environment R.TRP_Environment.

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

OE.SVD_Auth_CGA (CGA proves the authenticity of the SVD) is provided by FTP_ITC.1/SVD.IMPORT which assures identification of the sender and by FDP_UIT.1/ SVD IMPORT. which guarantees it's integrity.

OE.SCA_Trusted_Environment (Trusted environment of the SCA) is provided by R.TRP_Environment which protects (i) the confidentiality and integrity of the VAD entered by the user via the SCA human interface provided and sent to the TOE and (ii) the integrity of the DTBS sent by the SCA to the TOE in case the Trusted Path or Trusted Channel is not established by cryptographic means.

8.4 Depencency Rationale

8.4.1 Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled. The functional requirements dependencies for the TOE environment are not completely fulfilled (see section 8.4.2 for justification).

Table 8.5 : Functional and Assurance Requirements Dependencies
(the term 'see sub-section 6.4.2 for justification' shall be read as 'see sub-section 8.4.2 for justification')

Requirement	Dependencies
Functional Requirements	
FCS_CKM.1	FCS_COP.1/SIGNING, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1/ CORRESP	FDP_ITC.1/DTBS, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1/ SIGNING	FDP_ITC.1/DTBS, FCS_CKM.1, 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	FDP_ACF.1/Signature Creation SFP
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	FDP_ACC.1/Signature-Creation SFP, FMT_MSA.3
FDP_ACF.1/ SVD Transfer SFP	FDP_ACC.1/SVD Transfer SFP, FMT_MSA.3
FDP_ETC.1/ SVD Transfer SFP	FDP_ACC.1/ SVD Transfer SFP
FDP_ITC.1/DTBS	FDP_ACC.1/ Signature-Creation SFP, FMT_MSA.3
FDP_UIT.1/ SVD Transfer	FTP_ITC.1/SVD Transfer, FDP_ACC.1/SVD Transfer SFP
FDP_UIT.1/ TOE DTBS	FDP_ACC.1/Signature_Creation SFP, FTP_ITC.1/DTBS Import
FIA_AFL.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/Administrator	FDP_ACC.1/Initialisation SFP, FMT_SMR.1 FMT_SMF.1

Requirement	Dependencies
FMT_MSA.1/ Signatory	FDP_ACC.1/ Signature_Creation SFP, FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/Personalisation SFP, FMT_SMR.1 FMT_MSA.1/Administrator, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1/Administrator, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1
FMT_SMR.1	FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_PHP.1	FMT_MOF.1
FPT_TST.1	FPT_AMT.1
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	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 (GGA)	
FCS_CKM.2/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FCS_CKM.3/CGA	unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SVD IMPORT	FTP_ITC.1/SVD IMPORT, unsupported dependencies, see sub-section 6.4.2 for justification ,
FTP_ITC.1/ SVD IMPORT	None
Functional Requirements for Signature creation application (SCA)	
FCS_COP.1/ SCA HASH	Unsupported dependencies, see sub-section 6.4.2 for justification
FDP_UIT.1/ SCA DTBS	FTP_ITC.1/ SCA DTBS, unsupported dependencies on FDP_ACC.1, see sub-section 6.4.2 for justification
FTP_ITC.1/ SCA DTBS	None
FTP_TRP.1/SCA	None

8.4.2 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 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FCS_CKM.3/ CGA	The CGA imports SVD via trusted cannel implemented by FTP_ITC.1/ SVD import. The FCS_CKM.1 is not necessary because the CGA does not generate the SVD. There is no need to destroy the public SVD and therefore FCS_CKM.4 is not required for the CGA. The security management for the CGA by FMT_MSA.2 is outside of the scope of this PP.
FDP_UIT.1/ SVD Import (CGA)	The access control (FDP_ACC.1) for the CGA is outside the scope of this PP.
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, 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 PP.

8.5 Security Requirements Grounding in Objectives

This Chapter covers the grounding that have not been done in precedent chapter

Table 8.6 : Functional and Assurance Requirements Dependencies

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	EAL 4, OT.Lifecycle_Security
ALC_LCD.1	EAL 4, OT.Lifecycle_Security
ALC_TAT.1	EAL 4, 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 Objectives for the Environment	
R.Administrator_Guide	AGD_ADM.1
R.Sigy_Guide	AGD_USR.1
R.Sigy_Name	OE.CGA_QCert
R.TRP_Environment	AGD_USR.1

8.6 Rationale for Extensions

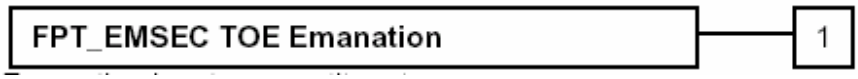
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations.

8.6.1 FPT_EMSEC TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE Emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FPT_EMSEC.1 TOE Emanation

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

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

Hierarchical to: No other components.

Dependencies: No other components.

8.7 Rationale for TOE Summary Specification

8.7.1 Rationale for TOE Security Functions

8.7.1.1 TOE Security Functions

The following table gives the coverage of the TOE Security Functional Requirements by the TOE Security Functions. The numbers in the table give the corresponding component of the Security Function covering the requirement, the identified components obviously satisfy the requirements.

Table 8-7 Functional Requirements to Security Function mapping

SFR / Security Function	SF.ACCESS	SF.ADMIN	SF.AUTH	SF.SIG	SF.CRYPTO	SF.TRUST	SF.PROTECTION	SF.IC_SF
FCS_CKM.1.1		3			4,6			
FCS_CKM.4.1/ RE-GENERATION		4						
FCS_COP.1.1/ CORRESP				4	1,2,4			3,4
FCS_COP.1.1/ SIGNING				3	1,2,4			3,4
FDP_ACC.1.1/ SVD Transfer SFP	3	1	1			3		
FDP_ACC.1.1/ Initialisation SFP	2	1	1			2		
FDP_ACC.1.1/ Personalisation SFP	4	1,7						
FDP_ACC.1.1/ Signature-creation SFP	5		1			2		4
FDP_ACF.1/ SVD Transfer SFP	3	1	1			3		

FDP_ACF.1/ Initialisation SFP	2	1	1			2		
FDP_ACF.1/ Personalisation SFP	4	1,7						
FDP_ACF.1/ Signature-creation SFP	5		1			2		
FDP_ETC.1/ SVD Transfer		6						
FDP_ITC.1/ DTBS				1				
FDP_RIP.1.1							1	
FDP_SDI.2/ Persistent					5		2	
FDP_SDI.2/ DTBS				2				
FDP_UIT.1/ SVD Transfer					3	3		4
FDP_UIT.1/ TOE DTBS					3	3		4
FIA_AFL.1			1					
FIA_ATD.1.1	1							
FIA_UAU.1	6		2					
FIA_UID.1	6		2					
FMT_MOF.1.1	7		3					
FMT_MSA.1.1/ Administrator	9	2						
FMT_MSA.1.1/ Signatory	8		2					
FMT_MSA.2.1		2	2			4		
FMT_MSA.3		5						
FMT_MTD.1.1	8		2					
FMT_SMF.1.1		2	2,3					
FMT_SMR.1	1							
FPT_AMT.1.1							3	
FPT_EMSEC.1							5	
FPT_FLS.1.1							6	
FPT_PHP.1								1
FPT_PHP.3.1								2
FPT_TST.1							4	
FTP_ITC.1/ SVD Transfer					4	1		3
FTP_ITC.1/ DTBS import					4	1		3
FTP_TRP.1/ TOE					4	1		3

8.7.2 Rationale for Assurance Measures

The following table demonstrates the coverage of the Assurance Requirements by the Assurance measures by indicating the correspondence with crosses.

Table 8-8 Assurance Requirements to Assurance Measures mapping

Assurance Requirements / Assurance Measures	AM_ACM	AM_ADO	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ACM	X						
ADO		X					
ADV			X				
AGD				X			
ALC					X		
ATE						X	
AVA							X

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 Rationale for Assurance Level 4 Augmented

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

AVA_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.

8.10 Rationale for PP Claims

Since the ST is only based on the SSCD PP [7], this part of the ST is omitted.

9 Conventions and Terminology

9.1 Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B “Specification of Protection Profiles”. Admissible algorithms and parameters for algorithms for secure signature-creation devices (SSCD) are given in a separate document [6]. Therefore, the ST refers to [6].

9.2 Terminology

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

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

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

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

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the SSCD for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair by the SSCD, if the requested SVD has not been generated by the SSCD yet. The CGA verifies the authenticity of the SVD by means of
(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. (defined in the Directive [1], article 2.11)

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

Data to be signed representation (DTBS-representation) means the data sent by the SCA to the TOE for signing and is
(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS. The SCA indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the SCA. The final hash-value in case (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 [1] is also referred to as the 'Directive' in the remainder of the PP.

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], 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 [1], 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 [1]. (SSCD is defined in the Directive [1], 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 [1], 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 (a) to perform the presentation of the DTBS to the signatory prior to the signature process according to the signatory's decision, (b) to send a DTBS-representation to the TOE, if the signatory indicates by specific nonmisinterpretable input or action the intend to sign, (c) 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 [1], 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 [1], article 2.7)

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

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

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

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

10 References

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

[2] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.

[6] Geeignete Kryptoalgorithmen In Erfüllung der Anforderungen nach §17 (1) SigG vom 22. Mai 2001 in Verbindung mit Anlage 1, I 2, SigV vom 22. November 2001, Bundesanzeiger Nr. 30, S.2537-2538, 13.02.04.

[7] Secure Signature-Creation Device Protection Profile Type 3, v1.05 EAL4+, BSI-PP-0006-2002, 25-July-2001

[8] Security Target Lite BSI-DSZ-CC-0244, Version 1.0, 15 October 2004, Evaluation of Philips P5CC036V1C Secure Smart Card Controller, Philips Semiconductors (sanitised public document)

[9] Smart Card IC Platform Version 1.0, Juli 2001, BSI-PP-0002-2001

[10] Reference has been removed. Enumeration not changed due to compatibility issues.

[11] Chipcards with digital signature application/function according to SigG and SigV, Part 4: Basic Security Services, DIN V66291-4, Final Draft, 07.06.2000

[12] PKCS#1: RSA Cryptography Stadard, Version 2.0, 1.10.1998

[13] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

[14] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.1999

[15] Certification Report, BSI-DSZ-CC-0311-2005 for Philips P5CC036V1C and P5CC009V1C Secure Smart Card Controller, Bundesamt für Sicherheit in der Informationstechnik, 12.09.2005

[16] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 32; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 02.07.2001, Final Interpretation 065, 31.07.2001

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

[18] Verordnung zur digitalen Signatur (Signaturverordnung) vom 16. November 2001

11 Acronyms

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy