Specification of the Security Target TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P

Version: 1.0.1/20111128

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	732 TCOS Signature Module Version 1.0 Release 1.doc
Stand:	28.11.2011
Version:	1.0.1
Hardware Basis:	SLE78CLX480P
Autor:	Ernst-G. Giessmann
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.0.1	2011-11-28	Final Document

Contents

1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils her requirements.

1.1 ST Reference

2

Title:	Specification of the Security Target TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P
TOE:	TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, T-Systems
CC Version:	3.1 (Revision 3)
Assurance Level:	EAL4 augmented.
General Status:	Final Version
Version Number:	1.0.1
Date:	2011-11-28
Certification ID:	BSI-DSZ-CC-732
Keywords:	Signature Module, Card Reader, tSign, PACE, EAC

1.2 TOE Reference

3 The Security Target refers to the Product “TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P” (TOE) of T-Systems for CC evaluation.

1.3 TOE Overview

4 The Target of Evaluation (TOE) addressed by the current Security Target is the smart card with contacts implementing a secure key store required by the Technical Guideline TR-03119, Version 1.1 [CRTR] for a card reader (Komfort-Chipkartenleser Cat-K), and a secure signature creation function. In the following it is called *Signature Module*.

5 The intended use for the TOE is restricted to this application in the infrastructure for the electronic identity card ePA and the reader should be familiar with the requirements for the Electronic ID Card ([ECARDTR]) as well as with the corresponding Protection Profile ([IDCARDPP]). During operational use phase there is only one User of the TOE, namely the card reader, where the Signature Module is integrated during the manufacturing of this card reader.

6 A more detailed description of the infrastructure will be given in chapter 3.3 Organizational Security Policies for the environment and in chapter4.2 for the Signature Module

Issuer as the general responsible, the ID Card Issuer and the CVCA supervising the Terminals, that use the TOE as a secure key store (Signature Module).

7 The TOE provides the following cryptographic algorithms and protocols to be used in the secure key store:

- Authentication of an external entity based on the PACE protocol;
- Encryption and authentication on a secure message channel;
- Secure digital signature creation with the stored secret key bound to the knowledge of authentication data (tSign-PIN).

8 The TOE is never used by an entity outside the Terminal (card reader). The signature creation, the secure channel and the authentication based on the PACE protocol is provided to the Terminal's software only. The 'Terminal Authentication' procedure requires that the Terminal generates a digital signature[1] over some protocol data. For that purpose the secret signature key stored in the TOE will be used. The signature can be created only if the Terminal's software authenticates as Signatory by authentication data called tSign-PIN.

9 To protect the tSign-PIN and the data to be signed all the communication between Terminal's software and the TOE is encrypted and protected by means of secure messaging. This secure channel is established by the well known and proven as secure PACE protocol executed between the Terminal's software and the TOE. It requires the knowledge of a secret, that may be even weak, but it establishes strong session keys. The derived key[2] is called PACE key. Note that this key is not related to the PACE protocol executed by the Terminal to establish a secure channel to the MRTD.

10 For CC evaluation only one application of corresponding product will be considered:

tSign Application similar to the *eSign* Application as specified in [EACTR, 3.1.3] containing data needed for generating terminal signatures. These signatures are neither advanced nor qualified electronic signatures because of lack of the signing person (Signatory [SSCDPP]). This application is intended to be used in the context of official and commercial services, where a signature of the Terminal as part of the Terminal Authentication protocol is required.

11 Therefore the Protection Profile [SSCDPP] is not applicable to the TOE and there is no conformance claim. Nevertheless from a technical viewpoint the signature function of the TOE fulfills almost all requirements of the Protection Profile [SSCDPP]. To support this view the requirements from the Protection Profile are copied into this ST and the text follows the corresponding notations. If there is no correspondence a different notation is used, e.g., SDSCD (secure digital signature creation device) instead of SSCD (secure signature creation device).

12 For the tSign Application, the Terminal acts as R.Sigy using secret Verification Authentication Data (tSign-PIN, i.e. VAD as specified in [SSCDPP, 3.2.3.5]).

13 The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure of the electronic ID cards. The security parameters of these algorithms must be selected by the Signature Module Issuer according to the Organizational Securi-

---

[1] denoted as s_{PCD} in [EACTR, section 4.4.1]

[2] denoted as K_{π}. in [EACTR, section 4.2]

ty Policies [IDCARDPP]. The TOE supports the standardized in RFC 5639 domain parameters mentioned in [ECARDTR, section 1.3.2] and the NIST P-256 curve mentioned in [EACTR2.03, A.2.1.1].

14 The Signature Module is integrated into a smart card of ID-000 format according to [ISO7810].

15 If in some context the hardware base is relevant, the TOE will be identified in more detail as the "TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P", otherwise the notion "TCOS Signature Module Version 1.0 Release 1" will be used, indicating that this context applies to any realization regardless which hardware base is used. The SLE78CLX480P chip is selected from the M7820 family. Note that the Chip Identifier Byte is not used in the TOE identification because it has no impact on the evaluation.

16 The TOE follows the composite evaluation aspects ([AIS36]). The Security Target of the underlying platform ([HWST]) claims conformance to Smartcard IC Platform Protection Profile ([PP0035]).

17 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [IDCARDPP] and the Life Cycle Model required by [PP0035] will be shown in 1.4.1.

1.4 TOE Description

1.4.1 TOE Definition

18 The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (operating system)
- the tSign Application and
- the associated guidance documentation

19 The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated files for the tSign Application in a file system. A detailed description of the parts of TOE will be given in other documents.

1.4.2 TOE security features for operational use

20 The following TOE security features are the most significant for its operational use:

- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal software acting as signer,
- Creation of digital signatures by the tSign Application,
- Self-protection of the TOE security functionality and the data stored inside.

21 These security features will be mapped to the security functions provided by the TOE in following chapter 7.

1.4.3 Non-TOE hardware/software/firmware

22 In order to be powered up and to communicate with the 'external world' the TOE needs a interface (internal card reader) supporting the communication protocol [ISO7816]. Note that this is an internal one connected only to the TOE and should not be confused with the card reader of the Terminal used for external ID cards.

1.4.4 Life Cycle Phases Mapping

23 Following the protection profile PP0035 [PP0035, sec. 1.2.3] the life cycle phases of a TCOS Signature Module device can be divided into the following seven phases[3]:

Phase 1: IC Embedded Software Development

Phase 2: IC Development

Phase 3: IC Manufacturing

Phase 4: IC Packaging

Phase 5: Composite Product Integration

Phase 6: Personalization

Phase 7: Operational Use

24 From a more abstract point of view (used e.g. in the PP [SSCDPP]) the TOE life cycle is described in terms of the following four life cycle phases.

Life cycle phase 1 "Development"

25 The TOE is developed in phase 1. The IC developer (i.e. the Platform Developer according to [AIS36]) develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

26 The software developer (i.e. the Application Developer according to [AIS36]) uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the dedicated applications and the guidance documentation associated with these TOE components.

27 The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories (EEPROM), the tSign Application and the guidance documentation is securely delivered to the Signature Module manufacturer.

28 This life cycle phase 1 covers Phase 1 and Phase 2 of [PP0035].

---

3 In the Protection Profile for Machine Readable Travel Documents with Extended Access Control ([EACPP3.1]) the phases are called s*teps*.

Life cycle phase 2 “Production” (Manufacturing)

29 In a first step the TOE integrated circuit is produced containing the TOE’s Dedicated Software and the parts of the Embedded Software in the non-volatile memories (ROM and EEPROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as Signature Module material during the IC manufacturing and the delivery process to the Signature Module manufacturer. The IC is securely delivered from the IC manufacturer to the Signature Module manufacturer (note that both of these roles may be assigned to different entities).

30 The Signature Module manufacturer

(i) add the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary,

(ii) creates the tSign Application, and

(iii) equips TOE’s chip with Pre-personalization Data and

(iv) packs the IC with contacts in the Signature Module.

31 The pre-personalized Signature Module together with the IC Identifier is securely delivered from the Signature Module manufacturer to the Personalization Agent. The Signature Module manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

32 This life cycle phase 2 corresponds to Phase 3 and Phase 4 of [PP0035] and may include for flexibility reasons Phase 5 and some production processes from Phase 6 as well. Depending on the requirements of the following Personalization life cycle phase 3 some restrictions for the file system may also be fixed already in this phase. Despite of that they all could be made also during Personalization, i.e. they are not changing the TOE itself, such an approach of delivering the TOE with different configurations is useful for terminal manufacturers. The mentioned restrictions fixed by the configuration never change the structure of the file system, but affect only the pre-allocation of maximal available memory and the a priori appearance of elementary files (EFs) for data groups to be allocated and filled up during Personalization. Note that any other file parameter including the access rules can not be changed.

33 The tSign Application is also already fixed in the file system; the applicable later on procedure activates it only and makes Signature Creation Data available as required by the tSign Application. Based on the Administrator Guidance [TCOSADM] the activating CSP develops a corresponding User Guidance for the tSign Application, which is delivered to the Signature Module holder by the CSP.

34 For the TOE one pre-configured version of the file system applies. A detailed description of the sub-phases and the file system pre-configurations, including file system identification and the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSADM].

35 The product is finished after initialization, after testing the OS and creation of the dedicated file system with security attributes and ready made for the import of User Data. This corresponds to the end of the life cycle phase 2 of the Protection Profile [EACPP3.1]. The TOE may also be pre-configured during manufacturing which leads to different configurations for delivering. A more detailed description of the production processes in Phases 5 and 6 of PP0035 [PP0035] is given in the Administrator Guidance document [TCOSADM].

Life cycle phase 3 “Preparation” (Issuing)

36 The personalization of the Signature Module consists of the writing of TOE User Data and TSF Data into the logical Signature Module. This includes the SCD.

37 The Password (Authentication Key) for Personalization is set during individually during Initialization and is delivered with the TOE to the Personalization Agent (for a detailed description see chap. 9 of Administrator Guidance [TCOSADM]).

38 The Personalization is performed by the Personalization Agent. If the Personalization is finished, the TSF Data can not be changed, the User Data (VAD) is in transport mode. The personalized Signature Module (together with appropriate guidance for TOE use if necessary) is handed over to the Terminal Manufacturer for operational use. The Terminal Manufacturer implements the Signature Module and sets the SCD operational.

39 This life cycle phase corresponds to the remaining initialization and personalization processes not covered yet from Phase 6 of the [PP0035].

40 *Application Note 1*: Note that from hardware point of view the life cycle phase “Issuing” is already an operational use of the composite product and no more a personalization of the hardware. The hardware’s “Personalization” (cf. [HWST]) ends with the initialization and pre-personalization of the TOE and should not be confused with the Personalization described in the Administrator Guidance [TCOSADM].

Life cycle phase 4 “Operational Use”

41 The TOE is used as Terminal’s secure key store by the terminal holder and the terminal’s software module.

42 This life cycle phase corresponds to the Phase 7 of the [PP0035].

43 The tSign Application is activated during Personalization, and only an authorized terminal (the User S.Admin according [SSCDPP]) can install the tSign key pairs. In the Operational Use phase the key generation is not available. The terminal’s certificate will be assigned to the Signature Module holder by the authorized terminal. No further Personalization procedure is required in Phase 7 (Operational Use).

44 The tSign Application is ready to use any of the installed tSign keys. Note that the Terminal Authentication fails, if the corresponding public key is not certified by CVCA.

45 The security environment for the TOE and the ST of the underlying platform match, the Phases up to 6 are covered by a controlled environment as required in [HWCR, p. 41]. In Phase 7 (Operational Use) no restrictions apply.

1.4.5 TOE Boundaries

1.4.5.1 TOE Physical Boundaries

46 Smart card as used in this ST means an integrated circuit containing a microprocessor, (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory which include RAM, ROM, and EEPROM.

47 The chip is embedded in a module which provides the capability for standardized connection to systems separate from the chip through contact interface in accordance with ISO standards.

48 The physical constituents of the TOE are the operating system, the data in elementary files of the dedicated file of the tSign Application (EEPROM), and temporary data used during execution of procedures associated to that dedicated file.

1.4.5.2 TOE Logical Boundaries

49 All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical boundaries of the TOE are given by the complete set of commands of the TCOS operating system for access, reading, writing, updating or erasing data.

50 The input to the TOE is transmitted over the physical interface as an octet string that has the structure of Command Application Protocol Data Unit (CAPDU).

51 The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

52 The Application Protocol Data Units or TCOS commands that can be used in the operating systems are described in more detail in another document.

2 Conformance Claim

2.1 CC Conformance Claims

53 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009,

Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009,

Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

54 as follows:

Part 2 extended,

Part 3 conformant.

55 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [CC] has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

2.2 PP Claims

56 This ST does not claim any conformance to any CC Protection Profile.

57 Nevertheless this ST follows the structure of Protection Profile for Electronic Identity Card (ID_Card PP), Version 1.03, BSI-PP-0061, 2009-12-15 [IDCARDPP] and the corresponding CC Protection Profile Secure Signature Creation Device – Part 2: Device with key generation, Version 1.03, BSI-PP-0059 [SSCDPP], to which strict conformance is claimed by the ID_Card PP.

2.3 Package Claims

58 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 5.

59 The evaluation assurance level of the TOE is EAL4 augmented with AVA_VAN.5 as defined in [CC].

2.4 Conformance Rationale

60 Because there is no conformance claim to a Protection Profile a rationale is not necessary.

61 Nevertheless the Security Problem Definition, the Security Objectives Statement and the Security Requirements Statement are related to those of the PP [SSCDPP].

3 Security Problem Definition

62 The ST covers only one application tSign related to the SPD statement of the TOE. This application corresponds to a signature application of an SSCD ([SSCDPP].). To allow an easier alignment in the following chapter the same notation is used.

3.1 Introduction

Assets

63 The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the Appendix Glossary for the term definitions)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
tSign			
1	user data stored on the TOE	All data (being not authentication data) stored in the Security Module being allowed to be *used* solely by the signer (the private signature key within the tSign Application). This asset is related to 'SCD' and 'DTBS-representation' in [SSCDPP].	Confidentiality[4] Integrity Authenticity
2	user data transferred between the TOE and the terminal containing the TOE	All data (being not authentication data) being transferred between the TOE and an authenticated terminal software. User data can be received and sent. This asset is related to 'DTBS' in [SSCDPP].	Confidentiality[4] Integrity Authenticity

Table 1: Primary assets

64 All these primary assets represent User Data in the sense of the CC.

65 The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	Asset	Definition	Property to be maintained by the current security policy
tSign			
3	Accessibility to the TOE functions and data only for authorized subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.	Availability
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way. Note that the authenticity of the TOE is related to the series that is equipped with the same secret key data.	Availability
5	TOE immanent secret cryptographic keys	Secret cryptographic material used by the TOE in order to enforce its security functionality[5].	Confidentiality

4 Though not each data element stored on the TOE represents a secret, anyway the specification [EACPP3.1] requires securing their confidentiality: only terminals authenticated according to [EACPP3.1, sec. 4.4] can get access to the user data stored.

Object No.	Asset	Definition	Property to be maintained by the current security policy
			Integrity
6	TOE immanent non-secret cryptographic keys	Non-secret cryptographic material used by the TOE in order to enforce its security functionality. This asset is related to 'SVD' in [SSCDPP].	Integrity Authenticity
7	Secret Signature Module holder authentication data	Secret authentication information being used for verification of the authentication attempts as authorized terminal software • derived PACE-Key • tSign-PIN (i) stored in the Signature Module[6] and (ii) transferred to it[7].	Confidentiality Integrity
8	Signature Module communication establishment authorization data	Authorization[8] information being used for verification of the authorization attempts as authorized user (derived PACE key). This data is stored in the TOE and are not to convey to it.	Confidentiality[8] Integrity

Table 2: Secondary assets

66 *Application Note 2*: Terminal software authentication and Signature Module communication establishment authorization data are represented by the same entity. Note that the password used for PACE is not to convey to the TOE.

67 The secondary assets represent TSF and TSF-data in the sense of the CC.

Subjects and external entities

68 Due to the technical correspondence of a Signature Module with an SSCD, the following roles are named corresponding to the SSCD descriptions, despite of the subjects are not natural persons but technical entities only.

69 This ST considers the following subjects:

External Entity	Subject	Role	Definition
1	1	Signature Module holder	An entity (a terminal of a series) for which the Signature Module Issuer has personalized the Security Module[9]. This subject corresponds to the 'S.Sigy' in [SSCDPP] and fulfills also the role of a terminal itself. Therefore other terminals are considered as subjects.
2	–	Signature Module user	The entity using a Signature Module, e.g. the terminal's software. This subject corresponds to 'S.User' in [SSCDPP]. Please note that a Signature Module User can also be an attacker (s. below).
3	–	Certification Service Provider (CSP)	An organization issuing certificates This entity corresponds to a Certification Service Provider in the sense of [SSCDPP] and the subject 'S.Admin' in [SSCDPP].

5 please note that the private signature key within the tSign Application (SCD) belongs to the object No. 1 'user data stored' above

6 is commensurate with RAD in [SSCDPP]

7 is commensurate with VAD in [SSCDPP]

8 Note that the PACE key data is not considered as restricted-revealable.

9 i.e. this entity is associated with a concrete electronic Signature Module Card

External Entity	Subject	Role	Definition
4	2	Personalization Agent	An organization acting on behalf of the Signature Module Issuer to personalize the Signature Module for the Signature Module holder by some or all of the following activities: (i) establishing the identity of the Signature Module holder, (v) writing the initial TSF data. Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the Signature Module Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role. This subject is commensurate with 'Personalization agent' in [EACPP3.1] and 'Administrator' in [SSCDPP].
5	3	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the Signature Module Manufacturer completing the IC to the Signature Module. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and Signature Module Manufacturer using this role Manufacturer. This subject is commensurate with 'Manufacturer' in [EACPP3.1].
6	4	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the [IDCARDPP], especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognized by the TOE. This subject corresponds to the 'Attacker' in [EACPP3.1] and [SSCDPP].

Table 3: Subjects

3.2 Threats

70 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE's use in the operational environment.

71 The threats defined in this ST are derived from the SSCD PP ([SSCDPP]).

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

72 An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during storage (import) and use for signature-creation in the TOE.

T.SCD_Derive Derive the signature-creation data

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

T.Hack_Phys Physical attacks through the TOE interfaces

74 An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

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

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

T.DTBS_Forgery Forgery of the DTBS/R

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

T.Sig_Forgery Forgery of the digital signature

77 Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. 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.

3.3 Organizational Security Policies

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

P.CSP_TCert Terminal certificate

79 The CSP uses a trustworthy CGA to generate a terminal certificate for the SVD generated for a terminal series during Personalization. The SVD matches the SCD implemented in the TOE.

P.TSign Secure digital signatures

80 The terminal uses a signature-creation application implemented in terminal's firmware to sign data with a secure digital signature. The DTBS is sent by the SCA as DTBS/R to the Signature Module. The Signature Module creates the digital signature created with a SCD implemented in the Signature Module that the terminal's firmware maintain under its control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SDSCD TOE as secure digital signature-creation device

81 The TOE ensures that: (a) the secrecy of the signature-creation data stored in the TOE and used for signature generation is reasonable assured; (b) the signature-creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; (c) the signature-creation data used for signature generation can be reliably protected against the use of attackers. The TOE does not alter the data to be signed and prevents such data from being presented to the signatory prior to the signature process.

This corresponds to the requirements an SSCD except that the SCD occur only once. Note that the SCD is assigned to a series of terminals.

P.Sig_Non-Repud Non-repudiation of signatures

82 The life cycle of the Signature Module, the SCD and the SVD shall be implemented in a way that the signature can not be denied to be created by one of a identified series of terminals as long as the terminal's certificate is not revoked.

83 The following Organizational Security Policies do not apply directly to the TOE but to the environment of the intended use. They are adopted from the ID_Card PP to indicate the requirements for the infrastructure, where the TOE is used.

P.Pre-Operational Pre-operational handling of the Signature Module

1. The Signature Module Issuer issues Signature Modules and approves terminals complying with all applicable laws and regulations.
2. The Signature Module Issuer guarantees the correctness of the user data (amongst other of those, concerning the Signature Module holder) and of the TSF-data permanently stored in the TOE[10].
3. The Signature Module Issuer uses only such TOE's technical components (IC) which enable traceability of the Signature Modules in their manufacturing and issuing life phases, i.e. *before* they are in the operational phase.
4. If the Signature Module Issuer authorizes a Personalization Agent to personalize the Signature Module for the Signature Module holder, the Signature Module Issuer has to ensure that the Personalization Agent acts in accordance with the Signature Module Issuer's policy.

P.Terminal_PKI PKI for Terminal Authentication (receiving branch)

84 *Application Note 3*: The description below states responsibilities of the involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1. The Signature Module Issuer shall establish a public key infrastructure for the card verifiable certificates used for terminal authentication. For this aim, the Signature Module Issuer shall run a domestic Country Verifying Certification Authority (domestic CVCA) and may use already existing foreign CVCAs[11]. The Signature Module Issuer shall make the CVCA Link Certificate available to the CSCA (who shall finally distribute it to its Signature Modules).
2. A CVCA shall securely generate, store and use the CVCA key pair. A CVCA shall keep the CVCA Private Key secret and issue a self-signed CVCA Certificate (C_{CVCA}) having to be made available to the Signature Module Issuer by strictly secure means as well as to the respective Document Verifiers. A CVCA shall create the Document

10 cf. Table 1 and Table 2 above

11 In this case there shall be an appropriate agreement between the ID_Card Issuer und a foreign CVCA ensuring enforcing the ID_Card Issuer's privacy policy. Existence of such an agreement may be technically reflected by means of issuing a C_{CVCA-F} for the Public Key of the foreign CVCA signed by the domestic CVCA.

Verifier Certificates for the Document Verifier Public Keys (C_{DV}) and distribute them back to the respective Document Verifier Verifiers[12].

3. A Document Verifier shall (i) generate the Document Verifier Key Pair, (ii) hand over the Document Verifier Public Key to the CVCA for certification, (iii) keep the Document Verifier Private Key secret and, (iv) securely use the Document Verifier Private Key for signing the Terminal Certificates (C_T) of the terminals being managed by him. The Document Verifier shall make C_T, C_{DV} and C_{CVCA} available to the respective Service Providers (who puts them in his terminals)[13].
4. A Service Provider shall (i) generate the Terminal Authentication Key Pairs {SK_{PCD}, PK_{PCD}}, (ii) hand over the Terminal Authentication Public Keys (PK_{PCD}) to the DV for certification, (iii) keep the Terminal Authentication Private Keys (SK_{PCD}) secret, (iv) securely use the Terminal Authentication Private Keys for the terminal authentication as defined in [EACTR], sec. 4.4 and (v) install C_T, C_{DV} and C_{CVCA} in the rightful terminals operated by him.

P.Trustworthy_PKI Trustworthiness of PKI

1. The CSCA shall ensure that it issues its certificates exclusively to the rightful organizations (DS) and DS shall ensure that they sign exclusively correct Card Security Objects having to be stored on the Signature Modules.
2. CVCAs shall ensure that they issue their certificates exclusively to the rightful organizations (DV) and DV shall ensure that they issue their certificates exclusively to the rightful equipment (terminals)[14].
3. CSPs shall ensure that they issue their certificates exclusively for the rightful data (public signature key of the Signature Module holder)[15].

P.Terminal Abilities and trustworthiness of rightful terminals

1. The rightful terminals (inspection system, authentication terminal and signature terminal shall be used by Service Providers and by Signature Module holders as defined in [EACTR], sec. 3.2.
2. They shall implement and use the terminal parts of the PACE protocol [EACTR], sec. 4.2, of the Terminal Authentication protocol [EACTR], sec. 4.4, of the Passive Authentication [EACTR], sec. 3.4 and of the Chip Authentication protocol [EACTR], sec. 4.3[16] and use them in this order[17]. A rightful terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

---

12 A CVCA shall also manage a Revocation Sector Key Pair {$SK_{Revocation}$, $PK_{Revocation}$} [EACTR], sec. 2.3 and 4.5.

13 A DV shall also manage a Revocation Sector Key Pair {$SK_{SectorNN}$, $PK_{SectorNN}$} [EACTR], sec. 2.3 and 4.5.

14 This rule is relevant for T.Skimming

15 This property is affine to P.CSP_QCert from [SSCDPP].

16 The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within [IDCARDPP] and is not supported by the TOE.

17 This order is only commensurate with the branch rightmost in Fig. 3.1, sec. 3.1.1 of [EACTR]. Other branches of this figure are not covered by the security policy of [IDCARDPP].

3. Rightful terminals shall store the related credentials needed for the terminal authentication (terminal authentication key pair {SK_{PCD}, PK_{PCD}} and the terminal certificate (C_T) over PK_{PCD} issued by the DV related as well as C_{DV} and C_{CVCA}; the terminal certificate includes the authorization mask (CHAT) for access to the data stored on the Signature Module) in order to enable and to perform the terminal authentication as defined in [EACTR], sec. 4.4.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of authenticity of PK_{PICC}, [EACTR], sec. 4.3.1.2).
5. A rightful terminal must not send assets (e.g. tSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the Chip Authentication after the Terminal Authentication.
6. A rightful terminal and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PIN, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

3.4 Assumptions

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

A.CGA Trustworthy certification-generation application

86 The CGA protects the authenticity of the Terminal's identification data and the SVD in the terminal's certificate by an secure digital signature (advanced electronic signature) of the CSP.

A.SCA Trustworthy signature-creation application

87 The terminal uses only a trustworthy SCA inside the firmware. The SCA generates and sends the DTBS/R of the data the Terminal have to sign in a form appropriate for signing by the TOE.

88 The Assumptions on security aspects of the environment derived from the hardware platform PP [PP0035] and the hardware platform ST [HWST] are considered in detail later in section 7.9.2 of the current ST.

A.SCD_Generate Trustworthy SCD/SVD generation

89 The Personalization Agent uses a Device for SCD/SVD generation that guarantees the cryptographic quality of the SCD/SVD pair.

90 The confidentiality of the SCD will be guaranteed by the Personalization Agent.

91 The SCD will not be used for signature-creation until the SCD is activated.

92 The generation of the SCD/SVD pair is invoked by authorized users only.

93 The Personalization Agent ensures the authenticity of the created SVD.

4 Security Objectives

94 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1 Security Objectives for the TOE

95 The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.

OT.Data_Integrity Integrity of Data

96 The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying).
The TOE must ensure integrity of the User Data during their exchange between the TOE and the Terminal's Software after the PACE Authentication.

OT.Data_Confidentiality Confidentiality of Data

97 The TOE must ensure the confidentiality of the User Data and the TSF-data by granting read access to authenticated users only.
The TOE must ensure confidentiality of the User Data during their exchange between the TOE and the Terminal's Software after the PACE Authentication.

OT.Lifecycle_Security Lifecycle security

98 The TOE shall detect flaws during the initialization, personalization and operational usage.

99 *Application Note 4*: The TOE may contain more than one SCD. There is no need to destroy the SCD in case of re-certification. Because the SCD is distributed over a series of terminals, it is impossible to destroy the SCD stored in one Signature Module.

OT.SCD_Auth_Imp Authorized SCD import

100 The TOE provides security features to ensure that authorized users only invoke the import of the SCD.

OT.SCD_Secrecy Secrecy of the signature-creation data

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

102 *Application Note 5*: The TOE shall keep the confidentiality of the SCD at all times in particular during SCD import, SCD signing operation and SCD storage.

OT.Sig_Secure Cryptographic security of the digital signature

103 The TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the

digital signatures or any other data exported from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF Signature creation function for the legitimate signatory only

104 The TOE provides the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

105 The TOE must not alter the DTBS/R This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

OT.EMSEC_Design Provide physical-emanation security

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

OT.Tamper_ID Tamper detection

107 The TOE provides system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.Tamper_Resistance Tamper resistance

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

109 The following TOE security objectives address the aspects of identified threats to be countered involving the TOE's environment.

OT.Identification Identification of the TOE

110 The TOE must provide means to store Initialization[18] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life phases of the Signature Module.

OT.Personalization Personalization of Signature Module

111 The TOE must ensure that the user data (amongst other those concerning the Signature Module holder) and the TSF-data permanently stored in the TOE can be written by authorized Personalization Agents only. The Card Security Object can be updated by authorized Personalization Agents (in the role of DS), if the related data have been modified. The *tSign Application* is installed on the TOE on behalf of the CSP taking the responsibility for this application.

18 amongst other, IC Identification data

4.2 Security Objectives for the Operational Environment

I. Signature Module Issuer as the general responsible

112 The Signature Module Issuer as the general responsible for the global security policy related will implement the following security objectives of the TOE environment:

OE.CGA_TCert Generation of terminal certificates

113 The CGA generates a terminal certificate according to [ECARDTR, sec. 2.2, p. 10].

114 The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in a secure digital signature creation device.

OE.SDSCD_Prov_Service Authentic SDSCD provided by SDSCD Provisioning Service

115 The SDSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalizes and delivers the TOE as SDSCD to the Signature Module holder.

OE.DTBS_Intend SCA sends data intended to be signed

116 The Signature Module User uses trustworthy SCA inside the firmware that

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

OE.DTBS_Protect SCA protects the data intended to be signed

117 The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

OE.Signatory Security obligation of the Signatory

118 The terminal manufacturer checks that the SCD stored in the Signature Module received from Signature Module manufacturer is in non-operational state. The terminal software keeps its VAD confidential.

OE.Personalization Personalization of the Signature Module[19]

119 The Signature Module Issuer must ensure that Personalization Agent acting on his behalf identifies the Signature Module to be personalized and writes the secret signature

19 This Security Objective for the Operational Environment covers other objectives mentioned e.g. in the Protection Profile [SSCDPP] or other related documents: Correspondence between SVD and SCD (OE.SCD_SVD_Corresp), Authorized SCD/SVD generation (OE.SCD/SVD_Auth_Gen), SCD Secrecy (OE.SCD_Secrecy), Authenticity of the SVD (OE.SVD_Auth) because the SCD/SVD Generation and the transfer to Signature Modules is available during Personalization only.

creation data. The Personalization Agent must ensure that the environment where the personalization of the Signature Module takes place guarantees that the authentication data of the Personalization Agent as well as all data transmitted during Signature Module personalization is protected against disclosure and modification. To meet the objective OT.Sig_Secure the Signature Module Issuer must ensure that the Personalization Agent uses only authentic SCD/SVD pairs of appropriate cryptographic strength. After SCD/SVD generation the SCD imported to the TOE will be protected by a Transport-PIN mechanism, which prevents the signature generation before the Signature Module is implemented in a terminal.

II. ID_Card Issuer and CVCA: Terminal's PKI (receiving) branch

120 The following objectives are related to the operational use phase of the Signature Modules. The ID_Card Issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the ID_Card Issuer Card Issuer)[20] will implement the following security objectives of the TOE environment:

OE.Terminal_Authentication Authentication of rightful terminals

121 The ID_Card Issuer has to establish the necessary public key infrastructure as follows: The domestic CVCA acting on behalf and according to the policy of the ID_Card Issuer as well as each foreign CVCA acting under agreement with the ID_Card Issuer and according to its policy must (i) generate a cryptographic secure CVCA Key Pair, (ii) ensure the secrecy of the CVCA Private Key and sign Document Verifier Certificates in a secure operational environment, (iii) make the Certificate of the CVCA Public Key (C_{CVCA}) available to the ID_Card Issuer, (who makes it available to his own CSCA[21]) as well as to the respective Document Verifiers, (iv) distribute Document Verifier Certificates (C_{DV}) back to the respective Document Verifiers. Hereby authenticity and integrity of these certificates are being maintained. A CVCA has also to manage a Revocation Sector Key Pair {$SK_{Revocation}$, $PK_{Revocation}$} [EACTR, sec. 2.3 and 4.5].
A Document Verifier acting in accordance with the respective CVCA policy must (i) generate a cryptographic secure Document Verifying Key Pair, (ii) ensure the secrecy of the Document Verifying Private Key, (iii) hand over the Document Verifier Public Key to the respective CVCA for certification, (iv) sign the Terminal Certificates (C_T) of the terminals being managed by him in a secure operational environment only, and (v) make C_T, C_{DV} and C_{CVCA} available to the respective Service Providers operating the terminals certified. This certificate chain contains, amongst other, the authorization level of pertained terminals for differentiated data access on the ID_Card [EACTR, sec. 2.3 and 4.5].
A Service Provider participating in this PKI (and, hence, acting in accordance with the policy of the related DV) must (i) generate the Terminal Authentication Key Pairs {SK_{PCD}, PK_{PCD}}, (ii) ensure the secrecy of the Terminal Authentication Private Keys, (iii) hand over the Terminal Authentication Public Keys {PK_{PCD}} to the DV for certification, (iv) securely use the Terminal Authentication Private Keys for the terminal authentication as defined in [EACTR], sec. 4.4 and (v) install C_T, C_{DV} and C_{CVCA} in the rightful terminals operated by him.
CVCAs must issue their certificates exclusively to the rightful organizations (DV) and DV must issue their certificates exclusively to the rightful equipment (terminals).

---

20 The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

21 CSCA represents the root of the issuing branch, see above.

OE.Terminal Terminal operating

122 The Service Providers participating in the current PKI (and, hence, acting in accordance with the policy of the related DV) must operate their terminals as follows:

1. They use their terminals (inspection systems, authentication or signature terminals) as defined in [EACTR], sec. 3.2.
2. Their terminals implement and use the terminal parts of the PACE protocol [EACTR], sec. 4.2, of the Terminal Authentication protocol [EACTR], sec. 4.4, of the Passive Authentication [EACTR], sec. 3.4 (by verification of the signature of the Card Security Object) and of the Chip Authentication protocol [EACTR], sec. 4.3[22] and use them in this order[23]. A rightful terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. Their terminals securely store the related credentials needed for the terminal authentication (terminal authentication key pair {SK_{PCD}, PK_{PCD}} and the terminal certificate (C_T) over PK_{PCD} issued by the DV related as well as C_{DV} and C_{CVCA}; the terminal certificate includes the authorization mask for access to the data stored on the ID_Card) in order to enable and to perform the terminal authentication as defined in [EACTR, sec. 4.4].
4. Their terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the ID_Card (determination of authenticity of PK_{PICC}, [EACTR, sec. 4.3.1.2]).
5. Their terminals and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PIN, integrity of PKI certificates and DTBS, etc.)

22 The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within the [IDCARDPP] and is not supported by the TOE.

23 This order is only commensurate with the branch rightmost in Fig. 3.1 [EACTR, sec. 3.1.1]. Other branches of this figure are not covered by the security policy of [IDCARDPP].

4.3 Security Objective Rationale

123 The following table provides an overview for security objectives coverage (TOE and its environment). It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	OT.Data_Integrity	OT.Data_Confidentiality	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.Identification	OT.Personalization	OE.CGA_TCert	OE.SDSCD_Prov_Service	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.Personalization	OE.Terminal_Authentication	OE.Terminal
T.SCD_Divulg					x														x		
T.SCD_Derive						x													x		
T.Hack_Phys					x				x	x	x										
T.SigF_Misuse	x	x	x				x	x								x	x	x	x		
T.DTBS_Forgery	x							x								x	x				
T.Sig_Forgery						x								x							
P.CSP_TCert			x	x										x					x		
P.TSign						x	x							x		x			x		
P.Sigy_SDSCD			x	x	x	x	x	x	x		x				x				x		
P.Sig_Non-Repud			x		x	x	x	x	x	x	x			x	x	x	x	x	x		
P.Pre-Operational												x	x						x		
P.Terminal																					x
P.Terminal_PKI																				x	
P.Trustworthy_PKI														x						x	
A.CGA														x					x		
A.SCA																x					
A.SCD_Generate																			x		

Table 4: Security Objective Rationale

124 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given below.

125 The OSP **P.Pre-Operational** is enforced by the following security objectives:

126 OT.Identification is affine to the OSP's property 'traceability before the operational phase'; OT.Personalization and OE.Personalization together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorization of Personalization Agents';

127 The OSP **P.Terminal** is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable.

128 The OSP **P.Terminal_PKI** is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal_Authentication.

129 The OSP **P.Trustworthy_PKI** is enforced by OE.Terminal_Authentication (for CVCA, receiving PKI branch) and by OE.CGA_TCert.

130 The rationale for the Organizational Security Policies, the Threats and the Assumptions related to the objectives is similar to that of [SSCDPP, chap. 8]. It is applied here since this ST does not claim conformance to the SSCD-PP.

131 **P.CSP_TCert** (CSP generates terminal certificates) establishes the CSP generating terminal certificate linking the terminal's hardware and the SCD implemented in the Signature Module under control of the terminal's signature application. P.CSP_TCert is addressed by the TOE security objective OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialization, personalization and operational usage, the security objective OE.Personalization of the environment, which requires the personalization environment to ensure the correspondence between the SVD and the SCD during their generation, and the security objective OE.CGA_TCert for generation of terminal certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE by an authorized import (OT.SCD_Auth_Imp).

132 **P.TSign** (signatures for Terminal Authentication) provides that the TOE and the SCA may be employed to sign authentication data. OE.Personalization ensures the protection of the SCD used by terminal's software and that certificates are issued for genuine terminals only. OT.Sigy_SigF addresses terminal’s software control of the SCD by requiring the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_TCert addresses the requirement of certificates building a base for the creation of signature for Terminal Authentication. The OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory (terminal) intends to sign.

133 **P.Sigy_SDSCD** (TOE as secure digital signature-creation device) requires the TOE to meet some properties of advanced electronic signatures. OT.SCD_Secrecy and OT.Sig_Secure ensure the secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_\ Resistance address specific objectives to ensure secrecy of the SCD against specific attacks; OT.SCD_Secrecy and OT.Sig_Secure ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE; OT.Sigy_\ SigF ensures that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others; OT.DTBS_Integrity_TOE ensures that the TOE does not alter the DTBS/R. The usage of SCD under control of the signatory (terminal) is ensured by OT.Lifecycle_Security requiring the TOE to detect flaws during the initialization, personalization and operational usage. OE.Personalization and OT.SCD_Auth_Imp limits the import of the SCD to authorized users only. OT.Sigy_SigF ensures that the TOE provides the signature generation function for the legitimate signatory only and that it protects the SCD against the use of others. OE.SDSCD_Prov_Service and OE.Personalization ensures that the signatory obtains a

TOE sample as an authentic, initialized and personalized SDSCD from an SDSCD provisioning service.

134 **P.Sig_Non-Repud** (Non-repudiation of signatures) deals with the acceptance of signed authentication data successfully verified with the SVD contained in the terminal's certificate. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensure the aspects of terminal's control over SCD. OE.SDSCD_Prov_Service ensures that the terminals use an authentic TOE, initialized and personalized for a series of terminals. OE.CGA_TCert ensures that the certificate allows to identify the terminal as one of a defined series and thus to link the SVD to the terminal. OE.Personalization and OE.CGA_TCert require the environment to ensure authenticity of the SVD as being linked to the TOE and used under control of the terminal. OE.Personalization ensures also that the SVD linked to the TOE corresponds to the SCD that is implemented in the TOE. OE.Signatory ensures that the terminal Manufacturer checks that the SCD, stored in the SDSCD received from an SDSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the terminals become into control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the terminal's signature creation application keeps the VAD confidential. OE.DTBS_\ Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE generates digital signatures only for a DTBS/R that the signature application has created to be signed. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature-creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

135 **T.SCD_Divulg** (Storing, copying, and releasing of the signature-creation data) addresses the threat against the validity of electronic signature due to storage and copying of SCD outside the TOE. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for digital signature creation and OE.Personalization ensuring the the trusted environment during Personalization.

136 **T.SCD_Derive** (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OE.Personalization counters this threat by implementing cryptographic secure generation of the SCD/SVD-pair and the protection of SCD in the secured operational environment during Personalization phase. OT.Sig_Secure ensures cryptographic secure digital signatures.

137 **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. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

138 **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 digital signatures by others than the intended signatory. OT.Data_Integrity and OT.Data_Confidentiality address the protection of user data (VAD) during transmission. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialization, personaliz-

ation and operational usage. OT.Sigy_SigF (Signature creation function for the intended signatory only) ensures that the TOE provides the signature-generation function for the intended signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory (terminal) intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.Signatory ensures that the terminal manufacturer checks that an SCD stored in the SDSCD when received from an SDSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the terminal becomes control over the SDSCD. OE.Signatory ensures also that the Signatory keeps the VAD confidential. OE.Personalization ensures the protection of SCD during Personalization and the selection of cryptographic strong parameters preventing a misuse of terminal authentication.

139 **T.DTBS_Forgery** (Forgery of the DTBS/R) addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS calculated by the signatory. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been built as DTBS, and by means of OE.DTBS_Protect, which ensures that the DTBS/R can not be altered in transit between the SCA and the TOE. The TOE supports that by the means of OT.Data_Integrity providing with non-relevant in this case OT.Data_Confidentiality a secure channel during transmission and by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

140 **T.Sig_Forgery** (Forgery of the digital signature) deals with non-detectable forgery of the digital signature. OT.Sig_Secure and OE.CGA_TCert address this threat in general. The OT.Sig_Secure (Cryptographic security of the digital signature) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. OE.CGA_TCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature.

141 **A.SCA** (Trustworthy signature-creation application) establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS for the data that has been presented to the Terminal and which the Terminal has to sign in a form which is appropriate for being signed by the TOE.

142 **A.CGA** (Trustworthy certification-generation application) establishes the protection of the assignment of the Certificate Holder Reference to the SVD in the terminal certificate by the CSP. This is addressed by OE.CGA_TCert (Generation of terminal certificates) and by OE.Personalization which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the TOE.

143 **A.SCD_Generate** (Trustworthy SCD/SVD generation) addresses the cryptographic quality of the generated keys. Whereas the TOE would be able to check some parameters the cryptographic strength must be ensured by the Signature Module Issuer or on its behalf by the Personalization Agent. This is addressed by OE.Personalization which ensures the cryptographic quality of the SCD that is implemented by the TOE. The Personalization Agent is required by OE.Personalization to protect the confidentiality of the generated SCD/SVD data and the authenticity of the SVD in the TOE. This includes the proof of authenticity of the SCD/SVD, generated by the Signature Module Issuer or on its

behalf by an authorized user. The protection by the Transport-PIN mechanism installed during Personalization ensures that the SCD can not be use used before activation.

144 For the Composite Evaluation the following Security Objectives for the Hardware Platform are relevant too. They are listed here for the sake of completeness only. The detailed analysis of the Security Objectives derived from the hardware platform ST [HWST] and the environment of the Hardware Platform is made separately in the chapter 7.9 (Statement of Compatibility).

145 The following Security Objectives for the Hardware Platform are based on [PP0035]:

O.Leak-Inherent	(Protection against Inherent Information Leakage)
O.Phys-Probing	(Protection against Physical Probing)
O.Malfunction	(Protection against Malfunctions)
O.Phys-Manipulation	(Protection against Physical Manipulation)
O.Leak-Forced	(Protection against Forced Information Leakage)
O.Abuse-Func	(Protection against Abuse of Functionality)
O.Identification	(TOE Identification)

146 They all will be shown being relevant and not contradicting the Security Objectives of the TOE. They will be mapped to corresponding objectives of the TOE.

147 The remaining objective O.RND is covered by Security Objectives OT.Data_Integrity, OT.Data_Confidentiality, OT.Sigy_SigF and the OE.DTBS_Intend. These Security Objectives of the TOE address the protection of data used for Signatory authentication, i.e. the confidentiality of transmitted data, and the integrity protection for the transmitted DTBS. Therefore this objective is supported by Security Objectives of the TOE.

5 Extended Components Definition

148 This protection profile uses components defined as extensions to CC part 2. All these extended components are drawn from Definitions of chapter 5 of [IDCARDPP].

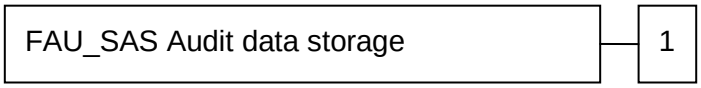
5.1 FAU_SAS Audit data storage

149 The family “Audit data storage (FAU_SAS)” is specified as follows.

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

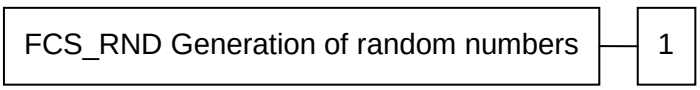
5.2 FCS_RND Generation of random numbers

150 The family “Generation of random numbers (FCS_RND)” is specified as follows.

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

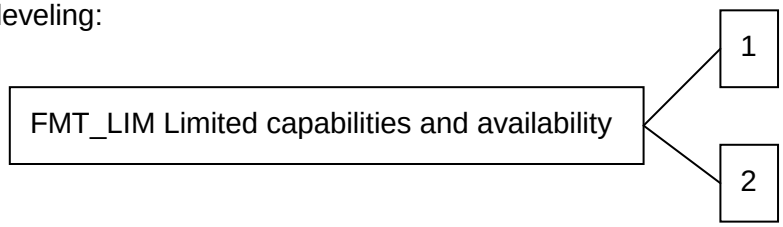
5.3 FMT_LIM Limited capabilities and availability

151 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:



FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) which are necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.2 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.1 Limited capabilities.

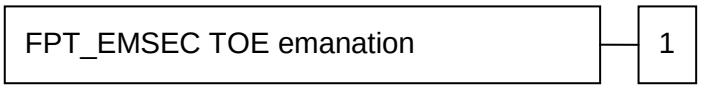
5.4 FPT_EMSEC TOE Emanation

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

FPT_EMSEC.1.2 Interface Emanation requires to 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 defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

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*].

Dependencies: No other components.

6 Security Requirements

152 This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

153 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

154 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

155 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made ST author appear underlined.

156 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments made by the ST author appear also underlined.

157 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.
For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

158 Some SFRs used this Security Target are inspired by SFRs from the Protection Profile for Secure Signature Creation Devices [SSCDPP]. The TOE itself is certainly not a SSCD as defined in this PP but it follows the requirements thereof. To indicate this the corresponding SFRs are denoted by '/SSCD' or '/xx_SSCD'.
This notation does not imply any conformance claim. It is used for information purposes only.

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

159 In order to give an overview of the security functional requirements mentioned in 1.4.2 in the context of the security services offered by the TOE, the author of the PP defined the security functional groups and allocated the functional requirements described in the following sections to them.

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	Supported by: – {FDP_ACC.1/Signature_Creation_SFP, FDP_ACF.1/Signature_Creation_SFP} – FDP_SDI.2/Persistent_SSCD – FMT_MTD.1/Signatory_SSCD, FMT_MSA.2/SSCD, FMT_MSA.3/SSCD , FMT_MSA.4/SSCD

Security Functional Groups	Security Functional Requirements concerned
Secure data exchange between the Signature Module and the Terminal containing the TOE	Supported by: – FCS_COP.1/AES: encryption/decryption – FCS_COP.1/CMAC: MAC generation/verification – FCS_CKM.1/DH_PACE, FCS_CKM.2/DH, FCS_COP.1/SHA, FCS_RND.1 – FTP_ITC.1/PACE, FDP_SDI.2/DTBS_SSCD – FIA_AFL.1/PACE
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT) – FIA_UAU.1/PACE: PACE Authentication (PCT) – FIA_UAU.4: single-use of authentication data – FIA_UAU.5: multiple authentication mechanisms – FIA_UAU.6: Re-authentication of Terminal – FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using non-blocking authentication and authorization data – FIA_UID.1/SSCD: Identification of Signature Module holder as Signatory (tSign-PIN) – FIA_UAU.1/SSCD: Authentication of Signature Module holder as Signatory (tSign-PIN) – FIA_SOS.1/SSCD: Specification of minimal tSign-PIN length Supported by: – FCS_CKM.1/DH_PACE: PACE authentication (PCT) – FCS_CKM.2/DH: Diffie-Hellmann key distribution within PACE – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_COP.1/SHA: Keys derivation – FCS_RND.1: random numbers generation – FTP_ITC.1/PACE: maintaining the secure channel after successful PACE authentication – FMT_SMR.1: security roles definition.
Audit	– FAU_SAS.1: Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialization and Pre-personalization – FMT_MTD.1/INI_DIS: Disabling access to Initialization and Pre-personalization Data in the operational phase
Generation of random numbers	– FCS.RND.1: Quality metric for random numbers
Creation of Digital Signatures by the tSign Application	– FCS_COP.1/SSCD
Management of and access to TSF and TSF-data	– The entire class FMT Supported by: – the entire class FIA: user identification/authentication During Personalization phase only – {FDP_ACC.1/SCD_Import_SFP, FDP_ACF.1/SCD_Import_SFP} – FDP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SCD
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT – FDP_RIP.1: enforced memory/storage cleaning – FDP_SDI.2/Persistent_SSCD – FDP_SDI.2/DTBS_SSCD Supported by: – the entire class FMT.

Table 5: Security functional groups vs. SFRs

160 The following table provides an overview of the keys and certificates used:

Name	Data
Receiving PKI branch	
Terminal Certificate (C_T)	The Terminal Certificate (C_T) is issued by the Document Verifier. It contains (i) the Terminal Public Key (PK_T) as authentication reference data, (ii) the coded access control rights of the terminal (EIS, ATT, SGT), the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal (PCT) as result of the PACE Protocol, see [EACTR], sec. A.3, F.2.3.
Signature keys	
Signature Creation Key Pair (SCD/SVD)	Signature Creation Data (SCD) is represented by a private cryptographic key being used by the Signature Module holder (signatory) to create an electronic signature. Signature Verification Data (SVD) is represented by a public cryptographic key corresponding with SCD and being used for the purpose of verifying an electronic signature. Properties of this key pair shall fulfill the relevant requirements stated in [ALGO] in order to be compliant with the German Signature Act.

Table 6: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

161 FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman Keys for PACE

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.2/DH
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/ DH_PACE: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [ECCTR][24] and specified cryptographic key sizes 256, 320, 384 and 512 bit length group order[25] that meet the following: [EACTR], Appendix A.3[26].

162 *Application Note 6:* The TOE generates a shared secret value with the terminal during the PACE Protocol, see [EACTR], sec. 4.2 and A.3. The shared secret value is used to derive the AES session keys for message encryption and message authentication

24 [assignment: *cryptographic key generation algorithm*]/[selection: *Diffie-Hellman-Protocol compliant to PKCS#3*, *ECDH compliant to* [ECCTR]]
25 [assignment: *cryptographic key sizes*]
26 [assignment: *list of standards*]

(PACE-K_{MAC}, PACE-K_{Enc}) according to [EACTR], F.2.3 for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

163 The following iterations are caused by other cryptographic key operation algorithms to be implemented by the TOE.

164 FCS_CKM.2/DH Cryptographic key distribution – Diffie-Hellman

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.2.1/DH The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the list below[27] that meets the following:

1. PACE: as specified in [EACTR, sec. 4.2 and A.3];[28].

165 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with zeros, random numbers or the new key[29] that meets the following: none[30].

166 *Application Note 7:* This SFR applies to the Session Keys, i.e. the TOE shall destroy the PACE Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. This SFR applies not to the Signature Key SCD. The Signature Creation Data can not be changed. Because the SCD is used for authentication purposes only a key destruction is not necessary. As soon as the corresponding certificate expires the Terminal Authentication will fail. Either the key will be re-certified or a new key will be selected. In both cases the SCD destruction is not required.

27 [assignment: *cryptographic key distribution method*]
28 [assignment: *list of standards*]
29 [assignment: *cryptographic key destruction method*]
30 [assignment: *list of standards*]

167 FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: not fulfilled, but justified: A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here. FCS_CKM.4 Cryptographic key destruction: not fulfilled, but justified: A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.
FCS_COP.1.1/ SHA	The TSF shall perform hashing[31] in accordance with a specified cryptographic algorithm SHA-1, SHA-224 and SHA-256 [32] and cryptographic key sizes none[33] that meet the following: FIPS 180-2 [34].

168 *Application Note 8:* Within the normative Appendix F of [EACTR, sec.F.2.3.1] 'Key Derivation' states that for deriving 128-bit AES keys the hash function SHA-1, whereas for deriving 192-bit and 256-bit AES keys SHA-256 shall be used.

169 The following iterations are caused by other cryptographic algorithms to be implemented by the TOE.

170 FCS_COP.1/AES Cryptographic operation – Encryption/Decryption AES

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/ AES	The TSF shall perform secure messaging – encryption and decryption[35] in accordance with a specified cryptographic algorithm AES in CBC mode[36] and cryptographic key sizes 128, 192 and 256 bit[37] that meet the following: FIPS 197 [FIPS197] and [EACTR] Appendix F.2.2[38].

31 [assignment: *list of cryptographic operations*]
32 [assignment: *cryptographic algorithm*]
33 [assignment: *cryptographic key sizes*]
34 [assignment: *list of standards*]
35 [assignment: *list of cryptographic operations*]
36 [assignment: *cryptographic algorithm*]

171 *Application Note 9:* This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of the transmitted data. The related session keys are agreed between the TOE and the terminal as part of either PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}). Note that in accordance with [EACTR] Appendix F.2.2 the (two-key) Triple-DES could be used in CBC mode for secure messaging. Due to the fact that (two-key) Triple-DES is not recommended anymore by the BSI (cf. [IDCARDPP]), Triple-DES is not applicable within operational use phase of the TOE.

172 FCS_COP.1/CMAC Cryptographic operation – CMAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]]; fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction:]; fulfilled by FCS_CKM.4.
FCS_COP.1.1/ CMAC	The TSF shall perform secure messaging – message authentication code[39] in accordance with a specified cryptographic algorithm CMAC[40] and cryptographic key sizes 128, 192 or 256 bit[41] that meet the following: [SP800-38B] and [EACTR] Appendix F.2.2[42].

173 *Application Note 10*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The related session keys are agreed between the TOE and the terminal as part of either PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with [EACTR] Appendix F.2.2 DES could be used in Retail mode for secure messaging. Due to the fact that Retail-MAC is not recommended anymore by the BSI (cf. [IDCARDPP]), this algorithm is not applicable within operational use phase of the TOE.

174 FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.

37 [assignment: *cryptographic key sizes*]/[selection: *128, 192, 256*]
38 [assignment: *list of standards*]
39 [assignment: *list of cryptographic operations*]
40 [assignment: *cryptographic algorithm*]
41 [assignment: *cryptographic key sizes*]/[selection: *128, 192, 256*] bit
42 [assignment: *list of standards*]

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet the quality requirements for SOF "high" according to [AIS31][43].

175 *Application Note 11*: This SFR requires the TOE to generate random numbers (random nonce) used for the PACE authentication protocol as required by FIA_UAU.4. Random numbers may also be required in the operational environment, e.g. for the Terminal Authentication.

176 **FCS_COP.1/SSCD Cryptographic operation – Digital Signature Generation**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: fulfilled by
FDP_ITC.1/SCD
FCS_CKM.4 Cryptographic key destruction]: not fulfilled, but justified:
Cryptographic key for Terminal Authentication expire with the corresponding certificate. A key destruction is not necessary.

FCS_COP.1.1/ SSCD The TSF shall perform digital signature generation[44] in accordance with a specified cryptographic algorithm ECDSA compliant to [ECCTR][45] and cryptographic key sizes 256, 320, 384 and 512 bit length group order[46] that meet the following: [ECCTR][47].

6.1.3 Class FIA Identification and Authentication

177 *Application Note 12:* The Table 7 provides an overview of the authentication mechanisms used.

Name	SFR for the TOE	Comments
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5 FIA_AFL.1/PACE	as required by FCS_CKM.1/DH_PACE
tSign-PIN	FIA_UAU.1/SSCD FIA_SOS.1/SSCD	No comment Replacement for the SSCD SFR FIA_AFL.1/SSCD

Table 7: Overview of authentication SFRs

43 [assignment: a defined quality metric]
44 [assignment: list of cryptographic operations]
45 [assignment: cryptographic algorithm]
46 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit
47 [assignment: *list of standards*]

178 **FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authentication/authorization data**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

FIA_AFL.1.1 The TSF shall detect when 1[48] unsuccessful authentication attempt~~s~~ occur**s** related to authentication attempt for PACE[49].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[50], the TSF shall require the restart of the PACE protocol.[51]

179 *Application Note 13*: The assignment operation reflects the fact that according the implementation the authentication procedure consumes a defined minimal amount of time. Because the derived PACE-Key possesses enough entropy for this reaction time (cf. Administrator Guidance [TCOSADM]), this is sufficient even to prevent a brute force attack with attack potential beyond high (to recover a random 10 digit number would require already about 300 years).

180 **FIA_UID.1/PACE Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE Protocol according to [EACTR], sec. 4.2[52]

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.

181 *Application Note 14:* The user identified after a successfully performed PACE protocol is the Terminal's Signature Application software (S.User), acting for the TOE like a PACE terminal. Note that this does not imply any identification as S.Admin or S.Sigy yet (cf. FIA_UAU.1/SSCD on p. 44). Nevertheless a secure channel between Terminal's Signa-

48 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]

49 [assignment: *list of authentication events*]

50 [selection: *met, surpassed*]

51 [assignment: *list of actions*]

52 [assignment: *list of TSF-mediated actions*]

ture Application software and the TOE protecting the transmission of DTBS and VAD is established.

182 *Application Note 15:* In the life phase 'Manufacturing' the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. Note that the TOE is not yet finished in this phase.
The Personalization Agent acts on behalf of the Signature Module Issuer under his and CSCA and DS policies. Hence, they define the requirements for Personalization Agents. The TOE supports the authentication of the Personalization Agent by a phase-specific authentication key. The TOE assumes the user role 'Personalization Agent', when the corresponding phase is reached and the terminal proves the knowledge of the Personalization Agent key.
The Configuration of the Signature Module related to the integration of the Signature Module in the Card Reader and is considered in FMT_SMF.1 (paragraph 220 on p. 52).

183 FIA_UAU.1/PACE Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE.
FIA_UAU.1.1/ PACE	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE Protocol[53] according to [EACTR, sec. 4.2][54] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/ PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

184 *Application Note 16:* Generally the user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). After a successfully performed PACE protocol the Terminal's Signature Application software is authenticated as S.User, acting for the TOE like a PACE terminal. Note that this does not imply any authentication as S.Admin or S.Sigy (cf. FIA_UAU.1/SSCD on p. 44).
If PACE was successfully performed, Secure Messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE, , which protects the transmission of DTBS and VAD.

185 FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminals by the TOE

Hierarchical to: No other components.

53 ID_Card identifies themselves within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

54 [assignment: *list of TSF-mediated actions*]

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to
1. PACE Protocol according to[EACTR], sec. 4.2. [55]

186 *Application Note 17:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed (the PP [IDCARDPP] supports the key derivation function based on AES; see [EACTR], sec. A.3.3 and F.2.1). For the TA protocol, in the operational environment a nonce r_{PICC} of 64 bits length is selected randomly, see [EACTR], sec. B.3 and B.11.6.

187 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide the General Authentication Procedure as the sequence
1. PACE Protocol according to [EACTR], sec. 4.2,

and
2. Secure messaging in encrypt-then-authenticate mode according to [EACTR], Appendix F[56]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. The TOE accepts the authentication attempt only if the terminal uses the PICC identifier[57] calculated during and the secure messaging established by the current PACE authentication.[58].

188 *Application Note 18:* The commands GET CHALLENGE and MSE:SET will be accepted even if they sent outside the SM channel. But in this case the channel will be closed and therefore all other commands with mandatory access control will not be accepted anymore.

189 FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

---

55 [assignment: *identified authentication mechanism(s)*]
56 [assignment: *list of multiple authentication mechanisms*]
57 ID_{PICC} = H(ephem-PK_{PICC}-PACE)
58 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the rightful terminal[59].

190 *Application Note 19:* The PACE Authentication Protocols as specified in [EACTR] start secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CMAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

191 FIA_UAU.1/SSCD Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/SSCD

FIA_UAU.1.1/ SSCD	The TSF shall allow 1. self test according to FPT_TST.1, 2. identification of the user by means of TSF required by FIA_UID.1/SSCD *3.* none[60] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/ SSCD	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

192 *Application Note 20*: This SFR is related to the signature related TSF-actions, i.e. to the authentication of S.Admin and S.Sigy and not to the actions in the PACE protocol (cf. FIA_UAU.1/PACE on p. 41). The iteration FIA_UAU.1/SSCD indicates this.

193 FIA_UID.1/SSCD Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/SSCD	The TSF shall allow 1. self test according to FPT_TST.1, *2.* none [61]

59 [assignment: *list of conditions under which re-authentication is required*]
60 [assignment: *list of (additional) TSF-mediated actions*]
61 [assignment: *list of additional TSF-mediated actions*]

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

194 *Application Note 21*: This SFR is related to the signature related TSF-actions, i.e. to the identification of S.Admin and S.Sigy and not to the actions in the PACE protocol (cf. FIA_UID.1/PACE on p. 41). The iteration FIA_UID.1/SSCD indicates this.

195 FIA_SOS.1/SSCD Specification of minimal tSign-PIN length

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1/SSCD	The TSF shall provide a mechanism to verify that secrets meet a minimal tSign-PIN length of 16 bytes[62].

196 *Application Note 22*: The SFR FIA_AFL.1/SSCD (Authentication failure handling) as used in the SSCD-PP [SSCDPP] is not considered in this ST because the RAD of the PIN is required to be chosen randomly and the length of the PIN is enforced to be at least 16 bytes (cf. [TCOSADM]), which corresponds to a security level of 128 bits. For a human user intended by the SSCD Protection Profile [SSCDPP] the SFR FIA_AFL.1 is essential due to a shorter length of the RAD. For a Signature Module that is used by the terminal's software this requirement gives no additional value because brute force attacks are computationally infeasible.

6.1.4 Class FDP User Data Protection

197 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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[63] the following objects: 1. the secret Signature Module holder authentication data tSign-PIN 2. the session keys (PACE-K_{MAC}, PACE-K_{Enc}) 3. the private signature key of the Signature Module holder (SCD)

62 [assignment: *a defined quality metric*]

63 [selection: *allocation of the resource to, de-allocation of the resource from*]

4. none[64].

198 *Application Note 23*: The functional family FDP_RIP possesses such a general character, so that is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMSEC.

199 *Application Note 24*: Please note that FDP_RIP.1 also contributes to achievement of OT.Sigy_SigF (tSign-PIN) and OT.SCD_Secrecy (SCD) from [SSCDPP].

200 The following security attributes and related status for the subjects and objects defined in the SSCD PP [SSCDPP] are applicable in this ST as well:

Subject / Object	Security attribute type	Values of the attribute
S.User	Role	R.Admin, R.Sigy
SCD	SCD Operational	no, yes
SCD	SCD Import allowed	no, yes
SCD	SCD Identifier	arbitrary value

201 *Application Note 25*: The Roles R.Admin and R.Sigy are not related to the roles Manufacturer, Personalization Agent and Signature Module holder. There may be even different entities taking over these roles. Therefore these roles should be maintained.

202 *Application Note 26*: The SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. This link is established during SCD/SVD Generation initiated by R.Admin and can not be changed later. The default value of the security attribute SCD Identifier is “NULL” (not assigned/not linked), i.e. the management function mentioned in no. 4 of FMT_SMF.1.1 is in fact an assignment and not really a change.

203 FDP_ACC.1/SCD_Import_SFP Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACC.1/SCD_Import_SFP

FDP_ACC.1.1/SCD Import_SFP	The TSF shall enforce the SCD Import SFP[65] on import of SCD by User[66].

204 FDP_ACF.1/SCD_Import_SFP Security attribute based access control

Hierarchical to: No other components.

64 [assignment: *list of objects*]
65 [assignment: *access control SFP*]
66 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Dependencies:	FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/Signature_Creation_SFP, FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCD

FDP_ACF.1.1/SCD Import_SFP	The TSF shall enforce the SCD Import SFP[67] to objects based on the following: 1. subjects: S.User associated with the attribute "Role", 2. objects: SCD with the attribute "SCD import allowed", 3. operations: import of SCD[68].
FDP_ACF.1.2/SCD Import_SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Administrator" is allowed to import SCD if the security attribute "SCD import allowed" is set to "yes"[69].
FDP_ACF.1.3/SCD Import_SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[70].
FDP_ACF.1.4/SCD Import_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: The user is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no"[71].

205 *Application Note 27*: The SCD Import is available only during Personalization. In this phase there in only one user, the R.Admin. If the Personalization is finished, the "SCD import allowed" attribute is set to "no". The Personalization phase is closed and can not be restarted. Therefore the SCD Import SFP adopted from [SSCDT2] is simplified and does not consider the User R.Sigy during SCD Import.

206 FDP_ACC.1/Signature_Creation_SFP Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACC.1/Signature_Creation_SFP

67 [assignment: *access control SFP*]

68 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

69 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

70 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

71 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1.1/ Signature_Creation_\ SFP	The TSF shall enforce the Signature_Creation_SFP[72] on 1. subjects: S.User, 2. objects: DTBS/R, SCD, 3. operations: signature-creation[73].

207 **FDP_ACF.1/Signature_Creation_SFP Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/Signature_Creation_SFP,
FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCD

FDP_ACF.1.1/ Signature_Creation_SFP	The TSF shall enforce the Signature_Creation_SFP[74] to objects based on the following: 1. the user S.User is associated with the security attribute "Role" and 2. the SCD with the security attribute "SCD Operational"[75].
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: R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[76].
FDP_ACF.1.3/ Signature_Creation_SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[77].
FDP_ACF.1.4/ Signature_Creation_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[78].

208 **FDP_SDI.2/Persistent_SSCD Stored data integrity monitoring and action**

72 [assignment: *access control SFP*]
73 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
74 [assignment: *access control SFP*]
75 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
76 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
77 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
78 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies

FDP_SDI.2.1/ Persistent_SSCD	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[79] on all objects, based on the following attributes: integrity checked stored data[80].
FDP_SDI.2.2/ Persistent_SSCD	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data 2. inform the S.Sigy about integrity error[81].

209 **FDP_SDI.2/DTBS_SSCD Stored data integrity monitoring and action**

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies

FDP_SDI.2.1/ DTBS_SSCD	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[82] on all objects, based on the following attributes: integrity checked stored DTBS[83].
FDP_SDI.2.2/ DTBS_SSCD	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data 2. inform the S.Sigy about integrity error[84].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1/SCD	The TSF shall enforce the SCD_Import_SFP[85] when importing user data controlled under the SFP form outside the TOE..
FDP_ITC.1.2/SCD	The TSF shall ignore any security attributes associated with the ~~user data~~ **SCD** when imported from outside the TOE
FDP_ITC.1.3/SCD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[86].

79 [assignment: *integrity errors*]
80 [assignment: *user data attributes*]
81 [assignment: *action to be taken*]
82 [assignment: *integrity errors*]
83 [assignment: *user data attributes*]
84 [assignment: *action to be taken*]
85 [assignment: *access control SFP*]
86 [assignment: *additional importation control rules*]

211 **FDP_UCT.1/SCD Basic data exchange confidentiality**

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1/SCD The TSF shall enforce the SCD_Import_SFP[87] to receive[88] ~~user data~~ **SCD** in a manner protected from unauthorized disclosure.

212 *Application note 28*: The user data relevant for SCD import is the SCD only.

6.1.5 Class FTP Trusted Path/Channels

213 **FTP_ITC.1/PACE Inter-TSF trusted channel after PACE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **Terminal after PACE** 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/PACE The TSF shall permit ~~another trusted IT product~~ **the Terminal**[89] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal after PACE[90].

214 *Application note 29*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}). The cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/AES and FCS_COP.1/CMAC. Note that the "Terminal" mentioned in FTP_ITC.1 is identified as the Terminal's Signature Application Software acting as a user.

215 **FTP_ITC.1/SCD Inter-TSF trusted channel**

87 [assignment: *access control SFP*]
88 [selection: *transmit, receive*]
89 [selection: *the TSF, another trusted IT product*]
90 [assignment: *list of functions for which a trusted channel is required*]

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SCD	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SCD	The TSF shall permit another trusted IT product[91] to initiate communication via the trusted channel.
FTP_ITC.1.3/SCD	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Personalization Terminal[92].

216 *Application note 30*: The trusted channel is established after successful performing the authentication of the Personalization Agent.

6.1.6 Class FAU Security Audit

217 FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1	The TSF shall provide the Manufacturer[93] with the capability to store the Initialization and Pre-Personalization Data [94] in the audit records.

218 *Application Note 31*: The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the Signature Module manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the Signature Module (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

91 [selection: *the TSF, another trusted IT product*]
92 [assignment: *list of functions for which a trusted channel is required*]
93 [assignment: *authorized users*]
94 [assignment: *list of audit information*]

6.1.7 Class FMT Security Management

219 *Application Note 32*: The SFRs FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

220 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Personalization,
3. Configuration[95].

221 *Application Note 33*: Initialization is the function of the Manufacturer, Personalization is assigned to the Personalization Agent and Configuration is done during the integration of the Signature Module in the Terminal. Note that since Initialization is done before the TOE is completed it might not be considered at all. Nevertheless this management function is already available during manufacturing and is assigned to the Manufacturer Role only. For further details refer to Administrator's Guidance [TCOSADM]. Configuration includes the activation of the SCD (cf. FMT_MSA.1/Signatory_SSCD on p. 56) The Card Reader Manufacturer acts in this case as S.Sigy and there is no need to consider it as an additional role. For further details refer to Administrator's Guidance [TCOSADM] too.

222 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Signature Module holder[96].

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

223 *Application Note 34*: For the explanation on the role Manufacturer please refer to the *Application Note 31*; on the role Personalization Agent – to the *Application Note 15*. The TOE recognizes the Signature Module holder by using PACE password (FIA_UID.1/ PACE) as well as – in the context of the tSign Application – by using SGT-implemen-

95 [assignment: *list of management functions to be provided by the TSF*]
96 [assignment: *the authorized identified roles*]

tation in the Terminal's firmware upon input VAD (tSign-PIN) governed by FIA_UAU.1/ SSCD.

224 *Application Note 35*: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

225 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced:

Deploying Test Features after TOE Delivery do not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. Embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[97].

226 FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:

Deploying Test Features after TOE Delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. Embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[98].

227 FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialization and Pre-personalization Data

Hierarchical to: No other components.

97 [assignment: *Limited capability and availability policy*]
98 [assignment: *Limited capability and availability policy*]

Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[99] the Initialization Data and Pre-personalization Data[100] to the Manufacturer[101].

228 **FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialization and Pre-personalization Data**

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to read out and to use[102] the Initialization Data[103] to the Personalization Agent[104].

229 *Application Note 36:* The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialization Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, the read and use access shall be blocked in the 'operational use' by the Personalization Agent, when he switches the TOE from the life phase 'issuing' to the life cycle phase 'operational use'. Please also refer to the *Application Note 15*.

230 *Application Note 37:* The following SFRs iterate the requirements given before. Note that those are related to the pre-usage phase and concern manufacturing, personalization and integration in the Terminal. The following iterations are related to the signature functionality only and concern the SCD import and the Transport-PIN creation by the Personalization Agent and the integration in the Terminal, enabling the signature function of the Signature Module.

231 **FMT_SMR.1/SSCD Security roles**

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/SSCD.

99 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
100 [assignment: *list of TSF data*]
101 [assignment: *the authorized identified roles*]
102 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
103 [assignment: *list of TSF data*]
104 [assignment: *the authorized identified roles*]

FMT_SMR.1.1/ SSCD	The TSF shall maintain the roles R.Admin and R.Sigy[105].
FMT_SMR.1.2/ SSCD	The TSF shall be able to associate users with roles.

232 FMT_SMF.1/SSCD Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1/ SSCD: The TSF shall be capable of performing the following management functions:

1. Creation and modification of RAD,
2. Enabling the signature-creation function,
3. Modification of the security attribute SCD operational,
4. Modification of the security attribute SCD import allowed,
5. Change the default value of the security attribute SCD Identifier,
6. none[106].

233 FMT_MOF.1/SSCD Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD
FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD.

FMT_MOF.1.1/ SSCD: The TSF shall restrict the ability to enable[107] the functions signature-creation function[108] to R.Sigy[109].

234 FMT_MSA.1/Admin_SSCD Management of security attributes

Hierarchical to: No other components.

105 [assignment: *the authorized identified roles*]
106 [assignment: *list of management functions to be provided by the TSF*]/[assignment: *list of other security management functions to be provided by the TSF*]
107 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
108 [assignment: *list of functions*]
109 [assignment: *the authorized identified roles*]

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/SCD_Import_SFP FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD
FMT_MSA.1.1/ Admin_SSCD	The TSF shall enforce the SCD_Import_SFP[110] to restrict the ability to modify[111] the security attributes SCD import allowed[112] to R.Admin[113].

235 **FMT_MSA.1/Signatory_SSCD Management of security attributes**

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/Signature_Creation_SFP FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD
FMT_MSA.1.1/ Signatory_SSCD	The TSF shall enforce the Signature_Creation_SFP[114] to restrict the ability to modify[115] the security attributes SCD operational[116] to R.Sigy[117].

236 *Application Note 38*: The security attribute “SCD operational” is set during Configuration by the Card Reader Manufacturer acting as S.Sigy using the commands “Change Reference Data” and “Reset Retry Counter”. It can not be changed later.

237 **FMT_MSA.2/SSCD Secure security attributes**

Hierarchical to:	No other components.

110 [assignment: *access control* SFP(s), *information flow control SFP(s)*]
111 [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]
112 [assignment: *list of security attributes*]
113 [assignment: *the authorized identified roles*]
114 [assignment: *access control* SFP(s), *information flow control SFP(s)*]
115 [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]
116 [assignment: *list of security attributes*]
117 [assignment: *the authorized identified roles*]

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/Signature_Creation_SFP and FDP_ACC.1/SCD_Import_SFP FMT_MSA.1 Management of security attributes: fulfilled by FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD
FMT_MSA.2.1/ SSCD	The TSF shall ensure that only secure values are accepted for SCD import allowed, SCD operational[118].

238 Application Note 39: The security attribute for setting the SCD import allowed is set to "yes" during Personalization and to "no" if the Personalization is finished. The security attribute for setting the SCD operational is set to "no" for the user S.Admin and to "yes" for the user S.Sigy.

239 FMT_MSA.3/SSCD Static attribute initialization

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes: fulfilled by FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD. FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD
FMT_MSA.3.1/ SSCD	The TSF shall enforce the SCD_Import_SFP, Signature_Creation_SFP[119] to provide restrictive[120] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/ SSCD	The TSF shall allow the R.Admin[121] to specify alternative initial values to override the default values when an object or information is created.

240 FMT_MSA.4/SSCD Security attribute value inheritance

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/SCD_Import_SFP, FDP_ACC.1/Signature_Creation_SFP
FMT_MSA.4.1/ SSCD	The TSF shall use the following rules to set the value of security attributes: If S.Admin successfully imports the SCD without S.Sigy being au-

118 [selection: *list of security attributes*]
119 [assignment: *access control SFP, information flow control SFP*]
120 [selection choose one of: *restrictive, permissive*, [assignment: *other property*]]
121 [assignment: *the authorized identified roles*]

thenticated the security attribute “SCD operational" of the SCD shall be set to “no” as a single operation.[122].

241 **FMT_MTD.1/Admin_SSCD Management of TSF data**

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD
FMT_MTD.1.1/ Admin_SSCD	The TSF shall restrict the ability to create[123] the RAD[124] to R.Admin[125].

242 **FMT_MTD.1/Signatory_SSCD Management of TSF data**

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/SSCD FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD
FMT_MTD.1.1/ Signatory_SSCD	The TSF shall restrict the ability to modify[126] the RAD[127] to R.Sigy[128].

243 Application Note 40: The implemented RAD for the tSign-PIN can not be changed, if the SCD is operational. It is fixed for concrete Signature Module in a concrete Terminal.

6.1.8 Class FPT Protection of the Security Functions

244 The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF-data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

---

122 [assignment: *rules for setting the values of security attributes*]
123 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
124 [assignment: *list of TSF data*]
125 [assignment: *the authorized identified roles*]
126 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
127 [assignment: *list of TSF data*]
128 [assignment: *the authorized identified roles*]

245 FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit power variations, timing variations during command execution [129] in excess of non-useful information [130] enabling access to

1. tSign-PIN[131]
2. none[132]

and

3. the private signature key of the Signature Module holder (SCD)[133].
4. none[134]

FPT_EMSEC.1.2 The TSF shall ensure any users[135] are unable to use the following interface Signature Module's circuit contacts[136] to gain access to

1. the tSign-PIN[137]
2. none[138]

and

3. the private signature key of the Signature Module holder (SCD)[139].
4. none[140].

246 *Application Note 41*: The TOE prevents attacks against the listed 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 be originated from internal operation of the TOE or may be caused 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 smart card. The Signature Module's chip has to provide contacts according to ISO/IEC 7810 ([ISO7810]).

247 FPT_FLS.1 Failure with preservation of secure state

129 [assignment: *types of emissions*]
130 [assignment: *specified limits*]
131 [assignment: *list of types of TSF data*]
132 [assignment: *list of types of (further) TSF data*]
133 [assignment: *list of types of user data*]
134 [assignment: *list of types of (further) user data*]
135 [assignment: *type of users*]
136 [assignment: *type of connection*]
137 [assignment: *list of types of TSF data*]
138 [assignment: *list of types of (further) TSF data*]
139 [assignment: *list of types of user data*]
140 [assignment: *list of types of (further) user data*]

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1
3. none [141].

248 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation[142] to demonstrate the correct operation of the TSF[143].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[144].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[145].

249 *Application Note 42*: The Signature Module's chip uses state of the art smart card technology, therefore it will run the some self tests at the request of an authorized user and some self tests automatically (cf. [HWST]). E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the user Manufacturer in the life phase 'Manufacturing'. Other self tests automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation of a integrity check value as soon as data is accessed.

250 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies

141 [assignment: *list of types of failures in the TSF*]
142 [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions* [assignment: *conditions under which self test should occur*]]
143 [selection: [assignment: *parts of TSF*], *the TSF*]
144 [selection: [assignment: *parts of TSF*], *TSF data*]
145 [selection: [assignment: *parts of TSF*], *TSF*]

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[146] to the TSF[147] by responding automatically such that the SFRs are always enforced.

251 *Application Note 43*: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

252 **FPT_PHP.1/SSCD Passive detection of physical attack**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2 Security Assurance Requirements for the TOE

253 The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following component:

- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

254 The following table provides an overview for security functional requirements coverage.

146 [assignment: *physical tampering scenarios*]
147 [assignment: *list of TSF devices/elements*]

	OT.Data_Integrity	OT.Data_Confidentiality	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.Identification	OT.Personalization
FCS_CKM.1/DH_PACE	x	x											
FCS_CKM.2/DH	x	x											
FCS_CKM.4	x	x											
FCS_COP.1/SHA		x											
FCS_COP.1/AES		x											
FCS_COP.1/CMAC	x												
FCS_RND.1	x	x											
FCS_COP.1/SSCD			x			x							
FIA_AFL.1/PACE	x	x											
FIA_UID.1/PACE	x	x											
FIA_UAU.1/PACE	x	x											
FIA_UAU.4	x	x											
FIA_UAU.5	x	x											
FIA_UAU.6	x	x											
FIA_UID.1/SSCD							x						
FIA_UAU.1/SSCD							x						
FIA_SOS.1/SSCD							x						
FDP_RIP.1							x						
FDP_ACC.1/SCD_Import_SFP			x	x									
FDP_ACF.1/SCD_Import_SFP			x	x									
FDP_ACC.1/Signature_Creation_SFP			x										
FDP_ACF.1/Signature_Creation_SFP			x										
FDP_SDI.2/Persistent_SSCD					x	x							
FDP_SDI.2/DTBS_SSCD							x	x					
FDP_ITC.1/SCD			x										
FDP_UCT.1/SCD			x		x								
FTP_ITC.1/PACE	x	x											
FTP_ITC.1/SCD			x		x								
FAU_SAS.1												x	x
FMT_SMF.1	x	x	x									x	x
FMT_SMR.1	x	x	x									x	x
FMT_LIM.1			x		x		x						
FMT_LIM.2			x		x		x						
FMT_MTD.1/INI_ENA			x									x	x
FMT_MTD.1/INI_DIS			x									x	x

	OT.Data_Integrity	OT.Data_Confidentiality	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.Identification	OT.Personalization
FMT_SMR.1/SSCD			x				x						
FMT_SMF.1/SSCD			x				x						
FMT_MOF.1/SSCD			x				x						
FMT_MSA.1/Admin_SSCD			x	x									
FMT_MSA.1/Signatory_SSCD			x				x						
FMT_MSA.2/SSCD			x	x			x						
FMT_MSA.3/SSCD			x				x						
FMT_MSA.4/SSCD			x	x			x						
FMT_MTD.1/Admin_SSCD			x				x						
FMT_MTD.1/Signatory_SSCD			x				x						
FPT_EMSEC.1					x				x		x		
FPT_FLS.1					x						x		
FPT_TST.1			x		x	x					x		
FPT_PHP.3			x		x						x		
FPT_PHP.1/SSCD										x			

Table 8: Coverage of Security Objectives for the TOE by SFR

255 The coverage of security objectives in this ST is related to [SSCDPP].

256 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

257 The security objective **OT.Identification** addresses the storage of Initialization and Pre-Personalization Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip.
This will be ensured by TSF according to SFR FAU_SAS.1.
The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_\ MTD.1/INI_DIS requires the Personalization Agent to disable access to Initialization and Pre-personalization Data in the life phase 'operational use'.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

258 The security objective **OT.Personalization** aims that only Personalization Agent can write the User- and the TSF-data into the TOE (it also includes installing/activating of the *tSign Application*).
This property is achieved requiring an appropriate authorization level during Personalization.
The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/ INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

259 The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and exchanged (physical manipulation and unauthorized modifying).
Physical manipulation is addressed by FPT_PHP.3.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
Unauthorized modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/CMAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).
The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

260 The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored exchanged.
This objective for the data stored is mainly achieved requiring a successful PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE), supported by FCS_CKM.1/ DH_PACE before any other access is granted. FDP_RIP.1 requires erasing the temporal values of tSign-PIN. FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used. The objective for the data exchanged is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/AES. The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for cryptographic operations needed and the SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

261 The security objective **OT.Lifecycle_Security** aims that the TOE shall detect flaws during the initialization, personalization and operational usage. This is achieved by the SCD_Import and Signature_Creation SFPs controlling the access rights (supported by the iterations of FDP_ACF.1 and FDP_ACF), the management functionalities (whole FMT group), the internal checks during signature creation (FCS_COP.1/SSCD) and the protection against physical attacks (FPT_PHP.3). The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ICT.1/ SCD. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

262 The security objective **OT.SCD_Auth_Imp** concerns the authorized SCD import. This is restricted to the Personalization phase and is available only once. This procedure is supported by the corresponding SFP and the requirements FDP_ACC.1/SCD_Import_\ SFP, FDP_ACF.1/ SCD_Import_SFP. The control of access rights is achieved by FMT_\ MSA.1/Admin_SSCD, FMT_MSA.2/SSCD and FMT_MSA.4/SSCD.

263 The security objective **OT.SCD_Secrecy** is provided by the security functions specified by FDP_UCT.1/SCD and FTP_ICT.1/SCD which ensures the confidentiality for SCD import. The test features necessary during initialization are no more available after TOE delivery (FMT_LIM.1, FMT_LIM.2). 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. The security functions specified by FDP_SDI.2/Persistent_SSCD ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. The SFRs FPT_EMSEC.1 and FPT_PHP.3/SSCD require additional security features of the TOE to ensure the confidentiality of the SCD.

264 The security objective **OT.Sig_Secure** is provided by the cryptographic algorithms specified by FCS_COP.1/SSCD, which ensure the cryptographic robustness of the signature

algorithms. FDP_SDI.2/Persistent_SSCD corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

265 The security objective **OT.Sigy_SigF** is provided by SFR for identification, authentication and access control. The FIA_UAU.1/SSCD and FIA_UID.1/SSCD ensure that signature generation can not be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin_SSCD and FMT_MTD.1/Signatory_SSCD manage the authentication function. The SFR FIA_SOS.1/SSCD provides protection against brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS_SSCD ensures the integrity of the stored DTBS. The security functions specified by FDP_ACC.1/Signature_Creation_SFP and FDP_ACF.1/Signature_Creation_SFP provide access control based on the security attributes managed by the SFRs FMT_MOF.1/SSCD, FMT_MTD.1/Signatory_SSCD, FMT_MSA.1/Signatory_\ SSCD, FMT_MSA.2/SSCD, FMT_MSA.3/SSCD and FMT_MSA.4/SSCD. FMT_SMF.1/ SSCD and FMT_SMR.1/SSCD list these management functions and the corresponding roles. This ensures that the signature process is restricted to the signatory. The test features necessary during initialization are no more available after TOE delivery (FMT_\ LIM.1, FMT_LIM.2). The security functions supporting FDP_RIP.1 ensure that any residual information on SCD is destroyed after the SCD has been use for signature creation.

266 The security objective **OT.DTBS_Integrity_TOE** aims that the DTBS-representation is not altered by the TOE. This is monitored by the TOE providing integrity functions specified by FDP_SDI.2/DTBS_SSCD.

267 The security objective **OT.EMSEC_Design** covers that no intelligible information is emanated. This is provided by FPT_EMSEC.1.

268 The security objective **OT.Tamper_ID** is provided by FPT_PHP.1/SSCD by the means of passive detection of physical attacks.

269 The security objective **OT.Tamper_Resistance** aims protection against disclosure of confidential User- or/and TSF-data stored on or processed by the TOE. This objective is achieved by FPT_EMSEC.1 for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, by FPT_FLS.1 and FPT_TST.1 against enforcing a malfunction of the TOE, and by FPT_PHP.3 for a detection of physical manipulation of the TOE.

6.3.2 Rationale for SFR's Dependencies

270 The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

271 The table below shows the dependencies between the SFR of the TOE.

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
1	FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_CKM.2/DH FCS_CKM.4
2	FCS_CKM.2/DH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/DH_PACE

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
		FCS_CKM.4	FCS_CKM.4
3	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1/DH_PACE
4	FCS_COP.1/SHA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	not fulfilled, but justified: hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here not fulfilled, but justified: A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here
5	FCS_COP.1/AES	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4
6	FCS_COP.1/CMAC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4
7	FCS_RND.1	No dependencies	n. a.
8	FCS_COP.1/SSCD	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FDP_ITC.1/SCD not fulfilled but justified: the SCD expires with its corresponding certificate, there is no need for key destruction
9	FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1/PACE
10	FIA_UID.1/PACE	No dependencies	n. a.
11	FIA_UAU.1/PACE	FIA_UID.1	FIA_UID.1/PACE
12	FIA_UAU.4	No dependencies	n. a.
13	FIA_UAU.5	No dependencies	n. a.
14	FIA_UAU.6	No dependencies	n. a.
15	FIA_UID.1/SSCD	No dependencies	n. a.
16	FIA_UAU.1/SSCD	FIA_UID.1	FIA_UID.1/SSCD
17	FIA_SOS.1/SSCD	No dependencies	n. a.
18	FDP_RIP.1	No dependencies	n. a.
19	FDP_ACC.1/SCD_Import_SFP	FDP_ACF.1	FDP_ACF.1/SCD_Import_SFP
20	FDP_ACF.1/SCD_Import_SFP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/SCD_Import_SFP FMT_MSA.3/SSCD
21	FDP_ACC.1/Signature_Creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature_Creation_SFP
22	FDP_ACF.1/Signature_Creation_SFP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signature_Creation_SFP FMT_MSA.3/SSCD
23	FDP_SDI.2/Persistent_SSCD	No dependencies	n. a.
24	FDP_SDI.2/DTBS_SSCD	No dependencies	n. a.

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
25	FDP_ITC.1/SCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import_SFP FMT_MSA.3/SSCD.
26	FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SCD FDP_ACC.1/SCD_Import_SFP
27	FTP_ITC.1/PACE	No dependencies	n. a.
28	FTP_ITC.1/SCD	No dependencies	n. a.
29	FAU_SAS.1	No dependencies	n. a.
30	FMT_SMF.1	No dependencies	n. a.
31	FMT_SMR.1	FIA_UID.1	FIA_UID.1/PACE, see also Application Note 34
32	FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
33	FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
34	FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
35	FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
36	FMT_SMF.1/SSCD	No dependencies	n. a.
37	FMT_SMR.1/SSCD	FIA_UID.1	FIA_UID.1/SSCD
38	FMT_MOF.1/SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1/SSCD
39	FMT_MSA.1/Admin_SSCD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1/SCD_Import_SFP FMT_SMF.1/SSCD FMT_SMR.1/SSCD
40	FMT_MSA.1/Signatory_SSCD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1/Signature_Creation_SFP FMT_SMF.1/SSCD FMT_SMR.1/SSCD
41	FMT_MSA.2/SSCD	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_ACC.1/SCD_Import_SFP and FDP_ACC.1/Signature_Creation_SFP FMT_MSA.1/Admin_SSCD and FMT_MSA.1/Signatory_SSCD FMT_SMR.1/SSCD
42	FMT_MSA.3/SSCD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin_SSCD and FMT_MSA.1/Signatory_SSCD FMT_SMR.1/SSCD
43	FMT_MSA.4/SSCD	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD_Import_SFP and FDP_ACC.1/Signature_Creation_SFP
44	FMT_MTD.1/Admin_SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1/SSCD
45	FMT_MTD.1/Signatory_SSCD	FMT_SMF.1	FMT_SMF.1/SSCD

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
		FMT_SMR.1	FMT_SMR.1/SSCD
46	FPT_EMSEC.1	No dependencies	n. a.
47	FPT_FLS.1	No dependencies	n. a.
48	FPT_TST.1	No dependencies	n. a.
49	FPT_PHP.3	No dependencies	n. a.
50	FPT_PHP.1/SSCD	No dependencies	n. a.

Table 9: Dependencies between the SFRs

272 The dependency analysis shows that all dependencies being expected by CC part 2 and by extended components definition (chapter 5) are either fulfilled or their non-fulfillment is justified.

6.3.3 Security Assurance Requirements Rationale

273 The current assurance package was chosen based on the pre-defined assurance package EAL4. This package 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 retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

274 The selection of the component AVA_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry ‘Attacker’). This decision represents a part of the conscious security policy for the Signature Module required by the Signature Module Issuer.

275 The set of *assurance* requirements being part of EAL4 fulfils all dependencies a priori.

276 The augmentation of EAL4 chosen comprises the following assurance component AVA_VAN.5. For this additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package.

6.3.4 Security Requirements – Internal Consistency

277 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

278 The analysis of the TOE’s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 6.3.2 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior of these 'shared' items.

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

279 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met, a possibility having been shown not to arise in sections 6.3.2 Rationale for SFR's Dependencies and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification

280 This section presents an overview of the security functionalities implemented by the TOE and the assurance measures applied to ensure their correct implementation.

281 According to the SFRs the TOE provides the following functionalities

- Access control to the User Data stored in the TOE
- Secure data exchange between the Signature Module and the terminal containing the TOE
- Identification and authentication of users and components
- Generation of random numbers
- Audit
- Creation of Digital Signatures by the tSign Application
- Management of and access to TSF and TSF-data
- Accuracy of the TOE security functionality / Self-protection

282 They are already mentioned in section 6.1.1 and implement the main security functions given in section 1.4.2:

- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal software acting as signer.

  This function is supported by Secure data exchange (7.2), Access control to the User Data stored in the TOE (7.1) and Identification and authentication of users and components (7.3).

- Creation of digital signatures by the tSign Application.

  This function is supported by Creation of Digital Signatures (7.6) and Identification and authentication of users and components (7.3).

- Self-protection of the TOE security functionality and the data stored inside.

  This function is supported by Reliability of the TOE security functionality (7.8).

- Audit is related to the pre-operational phase and is therefore not mentioned in section 1.4.2 as a security function of the operational phase

283 The TOE Summary Specification will be given in more detail in the following sections. Further technical information how the security functions actually implement the TOE security functional requirements, which TOE modules realize which functions is contained in the Security architecture Description (ADV_ARC), the Functional Specification (ADV_FSP) and the TOE Design Specification (ADV_TDS).

7.1 Access control to the User Data stored in the TOE

284 This Security Service is one of the main security services. It restricts and controls the access to user data stored in the TOE and provides the functionality of the secure key store required by [CRTR]. This function is also available in the pre-usage phase for the Manufacturer, the Personalization Agent and the Administrator. They use phase-specific keys for authentication, which are no more valid in the Operational Usage phase.

285 In the Operational Usage phase only one user, the Signatory will be accepted. It is the Terminal's software that authenticates by the means of the tSign-PIN. Note that additionally the TOE enforces a secure channel created after successfully executed PACE protocol (cf. chapter 7.2 Secure data exchange).

286 The access to User Data is restricted according to the SFRs FDP_ACC.1/Signature_\ Creation_SFP and FDP_ACF.1/Signature_Creation_SFP. The access control provided by this security function includes also the integrity check required by FDP_SDI.2/Persistent_SSCD for the stored signature key (SCD). The initialization of the security attributes is managed by SFRs FMT_MTD.1/Signatory_SSCD, FMT_MSA.2/SSCD, FMT_MSA.3/ SSCD and FMT_MSA.4/SSCD. These ensure that the signature process is restricted to the Signatory.

287 The modification of Authentication Data is not allowed. Each Signature Module has its own tSign-PIN, that is fixed after the SCD is set operational.

7.2 Secure data exchange

288 The TOE provides means for secure messaging which is required for all security related data exchange. The secure channel is established between the TOE and the Terminal that contains the TOE. The trusted channel is encrypted and integrity protected. The session keys are derived after PACE protocol executed between the TOE and Terminal's software.

289 The secure data exchange in a trusted channel is required by FTP_ITC.1/PACE. It is supported by fulfilling FCS_COP.1/AES giving confidentiality by data encryption/ decryption and FCS_COP.1/CMAC providing integrity. The quality and the authenticity of the key used based on the successful execution of the PACE protocol controlled by FIA_\ AFL.1/PACE. Note that despite of the password used in PACE may be weak nevertheless the trusted channel is protected by strong keys. This security function provides also the integrity check required by FDP_SDI.2/DTBS_SSCD for the transmitted DTBS.

290 The key agreement is supported by FCS_CKM.1/DH_PACE, FCS_CKM.2/DH, FCS_\ COP.1/SHA) and the quality of random numbers (FCS_RND.1) used by the Signature Module. For the security level of the used algorithms refer to the [EACTR].

7.3 Identification and authentication of users and components

291 This security service is available in the pre-usage phase, where the users are identified according to the corresponding phases as Manufacturer, Personalization Agent and Administrator. In the operational usage phase the Terminal's software is identified by using the PACE key. This allows for establishing the secure channel. The identification and authentication protocol PACE is described in the [EACTR], where the reliability and the security of the corresponding steps is considered and recognized as appropriate. Identification and authentication is provided for the Personalization Agent SDSCD related us-

ers, i.e. S.Admin and Terminal's Signature Creation Application software, (FIA_UID.1/ SSCD, FIA_UAU.1/SSCD).

292 The TOE itself must also be authenticated, which is supported by FIA_UID.1/PACE and FIA_UAU.1/PACE. The Requirements laid down in FIA_UAU.4, FIA_UAU.5 and FIA_\ UAU.6 concerns the protocol data, prevents re-use and how the security state, e.g. a specified role (FMT_SMR.1) of an identified and authenticated user or device is achieved and maintained. The re-identification and re-authentication for the subsequent communication use the means of the secure channel established after the PACE protocol is successfully executed (FTP_ITC.1/PACE).

293 The identification and authentication of the Signature Module holder as Signatory, i.e. the intention of the User to create an electronic signature, requires the successful verification of a tSign-PIN. It is not blocking because brute force attacks are computationally infeasible (FIA_SOS.1/SSCD). Due to the enforced minimal length of the tSign-PIN an authentication failure handling for the signature-creation is not required.

294 The security and the reliability of the identification and authentication is supported by the correct key agreement (FCS_CKM.1/DH_PACE, FCS_CKM.2/DH, FCS_COP.1/ SHA) and the quality of random numbers (FCS_RND.1) used by the Signature Module and the terminal. As the authentication state is left, the session keys can not be used anymore (FCS_CKM.4). If an unsuccessful authentication attempt occurs, the TOE reacts properly (FIA_AFL.1/PACE).

7.4 Audit

295 This security service is related to the Manufacturing and the Personalization phase.

296 The Manufacturer shall control the TOE production and must also file audit records (FAU_SAS.1). This is supported by FMT_MTD.1/INI_ENA (writing initialization and pre-personalization data) and is disabled for the Operational Phase (FMT_MTD.1/INI_DIS) by the Personalization Agent.

7.5 Generation of Random Numbers

297 The Random Number generation is a special service that is based on the security services of the underlying hardware. Therefore it is listed here separately.

298 The TOE uses random numbers for session key generation (FCS_RND.1). The Random Number Generator is provided by the Hardware (FCS_RNG.1 of [HWST]) and its cryptographic strength is ensured by the hardware evaluation. In case the operational environment needs random numbers, the TOE can provide them through the command specified in the ISO standard [ISO7816]. If the random numbers are provided by the TOE through a secure channel, the cryptographic quality is reliable.

7.6 Creation of Digital Signatures

299 The digital signature creation is the other main security service required by [CRTR]. The creation of terminal signatures must fulfill the strong requirements of [ECARDTR, sec. 2.2, p. 10]. The parameters for FCS_COP.1/SSCD are chosen according to this Technical Guideline.

300 From the technical point of view the TOE fulfills the requirement for a secure signature creation device according to [SSCDPP] except that the SCD is not assigned to a single user. This requirement is essential for an SSCD used by a human signatory but not for the authentication of a Card Reader to an Identity Card. Nevertheless the TOE provides strong cryptographic services for ECDSA signatures according to [ECARDTR].

7.7 Management of and access to TSF and TSF-data

301 The management and the access to the TOE security functions and the TSF data is controlled by the entire functionality class FMT. During Initialization, Personalization and in the Operational Phase of the Life Cycle Phases the Operation System of the TOE provides the management functions for identified roles (FMT_SMF.1, FMT_SMR.1, FMT_\ SMF.1/SSCD, FMT_SMR.1/SSCD) and maintain all the access rules over the life cycle of the TOE and even before the production of the TOE is finished during Initialization and Pre-Personalization (FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). During initialization necessary test features are no more available after TOE delivery (FMT_\ LIM.1, FMT_LIM.2).

302 The management and the access to TSF and TSF data in the pre-operational phase use secure messaging based on the authentication as Manufacturer and Personalization Agent (FMT_SMR.1, FIA_UAU.4, FIA_UAU.5), and the PACE protocol executed by the Card Terminal Manufacturer (FIA_AFL.1/PACE, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6). The Card Terminal Manufacturer, who incorporates the Signature Module in the Terminal, acts in this case as Signatory. Therefore it is not a separate role that must be considered.

303 The SCD user data are imported during Personalization phase by the Personalization Agent (in the R.Admin role) based on FMT_MSA.1/Admin_SSCD to enforce the SCD_\ Import_SFP (FDP_ACC.1/SCD_Import_SFP, FDP_ACF.1/SCD_Import_SFP) and can not be changed in the Operational Usage phase. The import is supported by FDP_\ ITC.1/SCD, FDP_UCT.1/SCD and FTP_ITC.1/SCD.

304 The tSign functionality can be accessed in the operational usage phase only. All the access rules and the memory assignment for the SCD is fixed during initialization phase and can not be changed later on, independent of the operational status of the application. The Administrator (R.Admin) creates the initial reference data objects (FMT_\ MSA.2/SSCD, FMT_MTD.1/Admin_SSCD). Thereafter only the Signatory is allowed to modify the security attribute "SCD operational" to "yes".

305 The successfully identified and authenticated User S.Sigy is able to set the SCD operational (FMT_MSA.1/Signatory_SSCD, FIA_UID.1/SSCD, FIA_UAU.1/SSCD). The security attributes "SCD import allowed" and "SCD operational" are monitored by the TOE (FMT_MSA.2/SSCD, FMT_MSA.3/SSCD, FMT_MSA.4/SSCD) during Personalization (SCD import allowed, but SCD not operational) and Configuration (SCD import not allowed and SCD is set operational). The strict sequence of Personalization and Configuration supports the enforcement of the SFRs.

306 After the SCD is set operational digital signatures can be created using the tSign functionality. The management functions of the Signatory, i.e. the Terminal's software, are more restricted than required. Even the Signatory is not allowed to change the RAD after the SCD is set operational (FMT_MTD.1/Signatory_SSCD). The change of the security attribute "SCD operational" to "yes" requires the authentication of the Signatory (FIA_\ UID.1/SSCD, FIA_UAU.1/SSCD). This is based on the transport PIN mechanism. Since the transport PIN is only known to the Signatory FMT_MOF.1/SSCD is enforced. The

transport PIN is changed by the Signatory to the tSign-PIN during Configuration. Thereafter the t-Sign-PIN will be card reader specific (FIA_UID.1/SSCD, FIA_UAU.1/SSCD) and the tSign functionality can only be used in the operational phase by the corresponding terminal's software.

307 The security of Signatory's authentication data is supported by the requirement of tSign-PIN length (FIA_UID.1/SSCD, FIA_UAU.1/SSCD, FIA_SOS.1/SSCD).

7.8 Reliability of the TOE security functionality

308 This security service is responsible for the protection of TSF, TSF and user data and the reliable function of the TSF.

309 The operating system of the TOE protects the security functionality of the TOE as soon as it it installed during Initialization Phase. The TOE will not emit physical or logical data information on security User Data outside the secure channels controlled by the operating system (FPT_EMSEC.1).

310 The TOE will resist physical manipulation and probing (FPT_PHP.1/SSCD, FPT_PHP.3) and enter a secure state in case a failure occur (FPT_FLS.1). This functionality is supported also by the hardware, which was approved in a separate evaluation process.

311 The TOE will permanently run tests to maintain the correct operation of the TOE security functions and the achieved security level (FPT_TST.1, FDP_SDI.2/Persistent_SSCD, FDP_SDI.2/DTBS_SSCD).

312 The TOE operating system controls the assignment of memory to the User Data in the file system and ensures that no information is available upon de-allocation of a resource. The access rules to the assigned memory remain the same even if the data is no more operational (FDP_RIP.1).

313 This functionality is supported by the entire class FMT.

7.9 Statement of Compatibility

314 This is the statement of compatibility between this Composite Security Target and the Security Target Chip of the underlying hardware [HWST].

7.9.1 Relevance of Hardware TSFs

315 The TOE is equipped with following Security Features to meet the security functional requirements:

Relevant:

- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

  Cryptographic support includes 3DES (not relevant), AES, RSA (not relevant), EC (not relevant), SHA-2 (SHA-256

and SHA512 – both not relevant), TRNG (relevant) and PRNG (not relevant).

Not relevant:

SF_DPM Device Phase Management

7.9.2 Compatibility: TOE Security Environment

Assumptions

316 The following list shows that assumptions neither of the TOE nor of the hardware have any conflicts between each other. They are either not relevant for this Security Target or are covered by appropriate Security Objectives.

Assumptions of the Composite ST: None

Assumptions related to the SSCD PP ([SSCDPP]):

A.CGA is covered by the Security Objectives for the TOE Environment OE.CGA_TCert and OE.Personalization.

A.SCA is covered by the Security Objectives for the TOE Environment OE.DTBS_Intend.

317 The identified here Objectives are related to OE.Personalization, that ensure the establishment of the correct identity of the Signature Module holder before the tSign Application is activated.

Assumptions of the Hardware PP ([PP0035]):

A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization) is not relevant, because the Personalization of the hardware is finished after Initialization Phase.

A.Plat-Appl (Usage of Hardware Platform) not relevant

A.Resp-Appl (Treatment of User Data) This assumption is covered by the hardware's objective for the environment OE.Resp-Appl which is related to TOE's Life Cycle Phase 1 "Development". It is supported by the Security Objectives OT.Data_Integrity, OT.Data_Confidentiality.

Assumptions of the specific hardware platform ([HWST]):

- A.Key-Function (Usage of Key-dependent Functions)

  Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to

leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). This assumption is covered by the Hardware‘s objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 “Development”.

Threats

318 The Threats of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Threats of the Composite ST:

- T.SCD_Divulg is related to Embedded Software Data and is therefore not relevant for treats of the hardware identified in the Smartcard IC PP [PP0035]
- T.SCD_Derive is related to Embedded Software Data and is therefore not relevant for treats of the hardware identified in the Smartcard IC PP [PP0035]
- T.Hack_Phys is related to the hardware and covers T.Leak_Inherent, T.Leak_Forced, T.Phys-Probing, T.Phys-Manipulation and T.Malfunction of the Smartcard IC PP [PP0035]
- T.SigF_Misuse is related to the Signature Function of the Embedded Software, but includes a threat related to the hardware, which is covered by T.Abuse_Func of the Smartcard IC PP [PP0035] and the entropy of random numbers used for signature creation (T.RND)
- T.DTBS_Forgery is related to the secure communication from the SCA to the TOE, depending on T.RND. Partially this threat includes also low level data integrity threats T.Phys_Manipulation, T.Abuse-Func from the Smartcard IC PP [PP0035] and T.Mem-Access from the hardware ST ([HWST].
- T.Sig_Forgery is related to robustness of the signature creation, depending on the entropy of random numbers provided by the hardware, i.e. T.RND.

Threats of the hardware ST ([PP0035]):

- T.Leak-Inherent is covered by T.Hack_Phys of the Composite ST
- T.Phys-Probing is covered by T.Hack_Phys of the Composite ST
- T.Malfunction is covered by T.Hack_Phys of the Composite ST
- T.Phys-Manipulation is covered by T.Hack_Phys of the Composite ST
- T.Leak-Forced is covered by T.Hack_Phys of the Composite ST
- T.Abuse-Func is covered by T.SigF_Misuse and T.DTBS_Forgery of the Composite ST

- T.RND is related to T.SigF_Misuse, T.DTBS_Forgery and T.Sig_Forgery of the Composite ST [SSCDPP]. An attacker predicting the output of the random number generator can manipulate the DTBS or break the security of the signature, misusing the TOE.

Threats of the hardware ST ([HWST]):

T.Mem-Access (Memory Access Violation)

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code) or privilege levels. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software. This threat is related to TOE's Life Cycle Phase 1 "Development". It is covered by the threat T.Abuse_Func of the TOE.

Organizational Security Policies

319 The Organizational Security Policies of the TOE and the hardware have no conflicts between each other. They are shown in the following list.

Organizational Security Policies of the Composite ST of the TOE:

- P.CSP_TCert no conflict
- P.TSign no conflict
- P.CSP_TCert no conflict
- P.Sigy_SDSCD no conflict
- P.Sig_Non-Repud no conflict
- P.Pre-Operational covers P.Process-TOE of the hardware ST
- P.Terminal no conflict
- P.Terminal_PKI no conflict
- P.Trustworthy_PKI no conflict

Organizational Security Policies of the Hardware ST:

- P.Add-Functions (Additional Specific Security Functionality) no conflict

  The TOE' hardware provides the following specific security functionality to the Smartcard Embedded Software: Advanced Encryption Standard, Triple Data Encryption Standard (not relevant), Rivest-Shamir-Adleman Cryptography (not relevant), Elliptic Curve Cryptography (not relevant), and Secure Hash Algorithm SHA-2.
- P.Process-TOE ([PP0035]) is covered by P.Pre-Operational of the Composite ST

Security Objectives

320 The Security Objectives of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Security Objectives for the Composite ST of the TOE related to the hardware:

- OT.Lifecycle_Security covers O.Add_Functions (AES) of the [HWST]
- OT.SCD_Secrecy covers O.Add_Functions (AES) of the [HWST]], O.Leak-Inherent and O.Leak-Forced from [PP0035]
- OT.Sig_Secure covers O.HW_AES of the [HWST]], O.Leak-Inherent and O.Leak-Forced from [PP0035]
- OT.Sigy_SigF covers O.Add_Functions (AES) of the [HWST]
- OT.DTBS_Integrity_TOE covers O.Add_Functions (AES) of the [HWST]
- OT.EMSEC_Design covers O.Leak-Inherent and O.Leak-Forced from [PP0035]
- OT.Tamper_ID covers O.Phys_Probing and O.Phys_Manipulation from [PP0035]
- OT.Tamper_Resistance covers O.Phys_Probing and O.Phys_Manipulation from[PP0035]
- OE.CGA_TCert is not relevant for the hardware of the TOE
- OE.SDSCD_Prov_Service is not relevant for the hardware of the TOE
- OE.DTBS_Intend is not relevant for the hardware of the TOE
- OE.DTBS_Protect is not relevant for the hardware of the TOE
- OE.Signatory is not relevant for the hardware of the TOE

Security Objectives for the hardware ([PP0035] and [HWST]):

- O.Leak-Inherent (Protection against Inherent Information Leakage) is covered by OT.Tamper_Resistance
- O.Phys-Probing (Protection against Physical Probing) is mapped to OT.Tamper_Resistance
- O.Malfunction (Protection against Malfunctions) is covered by the objectives OT.Sig_Secure and OT.Sigy_SigF
- O.Phys-Manipulation (Protection against Physical Manipulation) is mapped to OT.Tamper_ID and OT.Tamper_Resistance
- O.Leak-Forced (Protection against Forced Information Leakage) OT.EMSEC_Design
- O.Abuse-Func (Protection against Abuse of Functionality) is covered by the objective OT.Lifecycle_Security
- O.Identification (Hardware Identification) covered by OT.Identification, which is relevant for the pre-operational phases

- O.RND (Random Numbers) is covered by Security Objectives OT.Data_Integrity, and OT.Data_Confidentiality.

  The objectives of the TOE address the integrity and confidentiality of transmitted data, based on the protocols of Terminal and Chip Authentication, depending on a high cryptographic quality of random number generation.

- O.Add-Functions (Additional Specific Security Functionality)
- The hardware TOE must provide the following specific security functionality to the Smartcard Embedded Software: Advanced Encryption Standard (AES), which is mapped OT.Data_Integrity, and OT.Data_Confidentiality. The security functionality of Triple Data Encryption Standard), Rivest-Shamir-Adleman algorithm, Elliptic Curve Cryptography and Secure Hash Algorithm is not used and therefore not relevant.
- O.MEM_ACCESS is mapped to OT.Lifecycle_Security, OT.Sig_Secure

  This objective for the hardware supports the correct operation of the TOE providing control on restricted data or privilege levels.

Security Requirements

321 The relevant Security Requirements of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

Security Requirements of the Composite ST of the TOE:

- FCS_CKM.1/DH_PACE not relevant
- FCS_CKM.2/DH not relevant
- FCS_CKM.4 no conflicts
- FCS_COP.1/SHA no conflicts
- FCS_COP.1/AES matches FCS_COP.1/AES of [HWST]
- FCS_COP.1/CMAC no conflicts
- FCS_RND.1 matches FCS_RNG.1 of [HWST]
- FCS_COP.1/SSCD no conflicts
- FIA_AFL.1/PACE no conflicts
- FIA_UID.1/PACE no conflicts
- FIA_UAU.1/PACE no conflicts
- FIA_UAU.4 no conflicts
- FIA_UAU.5 no conflicts
- FIA_UAU.6 no conflicts
- FIA_UID.1/SSCD no conflicts
- FIA_UAU.1/SSCD no conflicts

- FIA_SOS.1/SSCD no conflicts
- FDP_RIP.1 no conflicts
- FDP_ACC.1/SCD-Import_SFP no conflicts
- FDP_ACF.1/SCD-Import_SFP no conflicts
- FDP_ACC.1/Signature_Creation_SFP no conflicts
- FDP_ACF.1/Signature_Creation no conflicts
- FDP_ITC.1/SCD not relevant
- FDP_UCT.1/SCD not relevant
- FTP_ITC.1/PACE not relevant
- FTP_ITC.1/SCD not relevant
- FAU_SAS.1 matches FAU_SAS.1 of [HWST]
- FMT_SMF.1 no conflicts
- FMT_SMR.1 not relevant
- FMT_LIM.1 matches FMT_LIM.1 of [HWST]
- FMT_LIM.2 matches FMT_LIM.2 of [HWST]
- FMT_MTD.1/INI_ENA not relevant
- FMT_MTD.1/INI_DIS not relevant
- FMT_SMF.1/SSCD no conflicts
- FMT_SMR.1/SSCD not relevant
- FMT_MOF.1/SSCD not relevant
- FMT_MSA.1/Admin_SSCD not relevant
- FMT_MSA.1/Signatory_SSCD not relevant
- FMT_MSA.2/SSCD not relevant
- FMT_MSA.3/SSCD not relevant
- FMT_MSA.4/SSCD not relevant
- FMT_MTD.1/Admin_SSCD not relevant
- FMT_MTD.1/Signatory_SSCD not relevant
- FPT_EMSEC.1 is supported by the Security Feature SF_PS of the hardware ([HWST]) and the AVA_VAN.5 evaluation
- FPT_FLS.1 matches FPT_FLS.1 of [HWST]
- FPT_TST.1 no conflicts
- FPT_PHP.3 matches FPT_PHP.3 of [HWST]
- FPT_PHP.1/SSCD is supported by FPT_PHP.3 of [HWST]

Security Requirements of the hardware

- FAU_SAS.1 covered by FAU SAS.1 of the Composite ST
- FCS_COP.1/AES covered by FCS_COP.1/AES of the Composite ST
- FCS_COP.1/DES not relevant, DES is not used in the OS, the same applies to FCS_COP.1/RSA, FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_COP.1/SHA which are not used

- FCS_RNG.1 (Quality metric for random numbers) matches FCS_RND.1 of the Composite ST
- FDP_ACC.1 (Subset access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF)
- FDP_ACF.1 (Security attribute based access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF
- FDP_ITT.1 (Basic internal transfer protection) is covered by FPT_EMSEC.1 of the Composite ST
- FDP_IFC.1 (Subset information flow control) is covered by FPT_EMSEC.1 of the Composite ST
- FMT_SMF.1 (Specification of Management Functions) is covered by FMT_SMF.1 of the Composite ST
- FMT_LIM.1 (Limited capabilities) is covered by FMT_LIM.1 of Composite ST
- FMT_LIM.2 (Limited availability) is covered by FMT_LIM.2 of Composite ST
- FMT_MSA.1 (Management of security attributes) no conflicts
- FMT_MSA.3 (Static attribute initialization) no conflicts
- FPT_FLS.1 (Failure with preservation of secure state) matches FPT_FLS.1 of the Composite ST
- FPT_ITT.1 (Basic internal TSF data transfer protection) is covered by FPT_EMSEC.1 of the Composite ST
- FPT_PHP.3 (Resistance to physical attack) is covered by FPT_FLS.1 and FPT_PHP.3 of the Composite ST
- FDP_SDI.1, FDP_SDI.2, FRU_FLT.2, FPT_TST.2 concern the hardware operation, no conflicts to SFRs of the TOE

Assurance Requirements

322 The level of assurance of the TOE is EAL 4 augmented with AVA_VAN.5

323 The chosen level of assurance of the hardware is EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5

324 This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

7.9.3 Conclusion

325 No contradictions between the Security Targets of the TOE and the underlying hardware can be found.

7.10 Assurance Measures

326 The documentation is produced compliant to the Common Criteria Version 3.1. The following documents provide the necessary information to fulfill the assurance requirements listed in section 6.2.

Development

ADV_ARC.1	Security Architecture Description TCOS Signature Module
ADV_FSP.4	Functional Specification TCOS Signature Module
ADV_IMP.1	Implementation of the TSF TCOS Signature Module
ADV_TDS.3	Modular Design of TCOS Signature Module

Guidance documents

AGD_OPE.1	User Guidance TCOS Signature Module
AGD_PRE.1	Administrator Guidance TCOS Signature Module

Life-cycle support

ALC_CMC.4, ALC_CMS.4	Documentation for Configuration Management
ALC_DEL.1	Documentation for Delivery and Operation
ALC_LCD.1	Life Cycle Model Documentation TCOS Signature Module
ALC_TAT.1, ALC_DVS.1	Development Tools and Development Security for TCOS Signature Module

Tests

ATE_COV.2, ATE_DPT.1	Test Documentation for TCOS Signature Module
ATE_FUN.1	Test Documentation of the Functional Testing

Vulnerability assessment

AVA_VAN.5	Independent Vulnerability Analysis TCOS Signature Module

327 The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

328 The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

329 The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

330 The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well-defined and use semi-formal methods, i.e. a security model.

331 The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at T-Systems International GmbH.

332 As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

Appendix Glossary and Acronyms

333 The glossary and the acronym's list are adopted from those of [IDCARDPP], more detailed information can be found there, too.

Glossary

Term	**Definition**
Advanced Electronic Signature	According to the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on “a Community framework for electronic signatures” a digital signature qualifies as an electronic signature, if it is: - uniquely linked to the signatory; - capable of identifying the signatory; - created using means that the signatory can maintain under his sole control, and - linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Agreement	This term is used in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application Note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the Signature Module’s chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm that the Signature Module itself and the data elements stored in were issued by the Signature Module Issuer
Basic Access Control	Security mechanism defined in [BACPP3.1] by which means the MRTD’s chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on MRTD’s chip according to LDS.
Certificate chain	Hierarchical sequence of Terminal Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Certification Service Provider (CSP)	An organization issuing certificates or providing other services related to electronic signatures. There can be CSP, who cannot issue qualified certificates (usually named ‘common’) or Qualified CSP, who issues qualified certificates. A CSP is the Certification Service Provider in the sense of [SSCDPP].
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means [ICAO9303-1].
CV Certificate	Card Verifiable Certificate according to [EACTR], appendix C.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Eavesdropper	A threat agent reading the communication between the Signature Module and the Terminal to gain the data on the Signature Module.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait. [ICAO9303-1]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO9303-1]

Term	**Definition**
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
Identity Card (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Identity Card is used in order to verify that identity claimed by the Identity Card presenter is commensurate with the identity of the Identity Card holder stored on/in the card.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO9303-1]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO9303-1]
Initialization Data	Any data defined by the Signature Module manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as IC_Card material (IC identification data).
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The Signature Module's chip is an integrated circuit.
Integrity	Ability to confirm the Signature Module and its data elements stored upon have not been altered from that created by the Signature Module Issuer.
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO9303-1]
Issuing State	The Country issuing the MRTD. [ICAO9303-1]
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO9303-1]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO9303-1] The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for both PACE and BAC.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO9303-1]
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the Signature Module Manufacturer completing the IC to the Signature Module. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and Signature Module Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [EACTR], sec. C.1.3. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorization Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE Terminal (PCT)	A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the Signature Module using a shared password (PACE password). The PCT is not allowed reading User Data (see sec. 4.2.2 in [EACTR]). See [EACTR], chap. 3.3, 4.2, table 1.2 and G.2.

Term	**Definition**
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card (Document) Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card (Document) Security Object. See [EACTR], sec. 1.1.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [EACTR], sec. 4.2. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personal Identification Number (PIN)	A short secret password being only known to the Signature Module holder (Card Terminal's software).
Personalization	The process by which the individual-related data are stored in a Signature Module. In the scope of this ST this applies to signature key pair(s) for the tSign Application.
Personalization Agent	An entity or organization acting on behalf of the Signature Module Issuer to personalize the Signature Module for the Signature Module holder by some or all of the following activities: (i) generating signature key pairs (SCD/SVD according to [SSCDPP]),(ii) writing the initial TSF data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalized Signature Module and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalized Signature Module's chip	Signature Module's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service Provider	An official or commercial organization providing services which can be used by the Terminal holder. Service Provider uses the rightful terminals managed by a DV.
tSign Application	A part of the TOE containing the non-executable data needed for generating digital signatures on behalf of the Signature Module Holder for authentication; this application is intended to be used in the context of services, where an digital signature of the Card Terminal containing the Signature Module is required.
Signature Module (electronic)	The contact based smart card integrated into the plastic and providing the tSign application.
Signature Module holder	The rightful Card Terminal (one of a series), for which the Signature Module Issuer personalized the Signature Module. This subject corresponds to the subject 'Signatory' in [SSCDPP] (cf. chapter 3.1).
Signature Module Issuer (issuing authority)	Organization authorized to issue a Signature Module to the Signature Module holder
Signature Module user	The entity using a Signature Module, e.g. the terminal's software. This subject corresponds to the subject 'User' in [SSCDPP] (cf. chapter 3.1).
Terminal	A technical system communicating with the TOE through the contactless interface.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
Unpersonalized Signature Module	Signature Module material prepared to produce a personalized Signature Module containing an initialized and pre-personalized Signature Module's chip.
User Data	All data (being not authentication data) stored in the context of the applications of the Signature Module. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC]).
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority (the PP author decided not to use the usual abbreviation 'CA' in order to avoid a collision with 'Chip Authentication')
DTBS	Data to be signed, please refer to [SSCDPP]
EAC	Extended Access Control
EIS	Extended Inspection System (equivalent to the Inspection Systems as defined in [EACTR], sec. 3.2)
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PCT	PACE-authenticated terminal
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
RAD	Reference Authentication Data, please refer to [SSCDPP]
RF	Radio Frequency
SAR	Security assurance requirements
SCA	Signature creation application, please refer to [SSCDPP]. It is equivalent to SGT in the current context.
SCD	Signature Creation Data, please refer to [SSCDPP]; the term 'private signature key within the tSign Application' is synonym
SDSCD	Secure digital signature creation device, this abbreviation is used for a device, that protects ist signature function like an SSCD, but is not an SSCD itself
SSCD	Secure signature creation device, evaluated and certified according to [SSCDPP]
SGT	Signature Terminal as defined in [EACTR], sec. 3.2
SVD	Signature Verification Data, please refer to [SSCDPP]
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functions
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data, please refer to [SSCDPP]

References

[AIS31]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Version 1 vom 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ALGO]

Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, 06.01.2010, Veröffentlicht am 04.02.2010 im Bundesanzeiger Nr. 19, S. 426

[BACPP3.1]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, BSI-PP-0055, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-29

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, July 2009, CCMB-2009-07-001,
Part 2: Security Functional Requirements; Version 3.1, July 2009, CCMB-2009-07-002,
Part 3: Security Assurance Requirements; Version 3.1, July 2009, CCMB-2009-07-003

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, July 2009, CCMB-2009-07-004

[CRTR]

Technische Richtlinie TR-03119: Anforderungen an Chipkartenleser mit ePA Unterstützung Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-12-15

[EACPP2.3]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.2, BSI-PP-0026, 2006-09-07

[EACPP3.1]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.10, BSI-PP-0056, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25

[EACTR]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.02, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-11-09

[EACTR2.03]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-03-24

[ECARDTR]

Technische Richtlinie TR-03116-2 für die eCard-Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, Stand 2010, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-04-28

[ECCTR]

Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-04-17

[FIPS180]

Federal Information Processing Standards Publication FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS), February 2004

[FIPS197]

Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[HWCR] Certification Report of the underlying hardware platform

BSI-DSZ-CC-0640-2010 for Infineon Technologies Smart Card IC (Security Controller) M7820 A11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-08-09

[HWST] Security Target of the underlying hardware platform

Security Target M7820 A11, Version 0.7, Infineon Technologies AG, Chipcard and Security, Evaluation Documentation, 2010-08-11

[ICAO9303-1]

ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, volume 2, ICAO, 6th edition, 2006

[IDCARDPP]

CC Protection Profile: Electronic Identity Card (ID_Card PP), Version 1.03, BSI-PP-0061, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-12-15

[ISO7810]

ISO/IEC 7810:2003, Identification cards – Physical characteristics, ISO, 2010-05-03

[ISO7816]

ISO 7816-4:2005, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2008-10-03

[ISO14443]

ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

[ISO15946]

ISO 15946, Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002

[PP0035]

Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007

[SP800-38B]

Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

[SSCDPP]

Protection Profiles for Secure Signature Creation Device – Part 2: Device with Key Generation, EN 14169-1:2009, ver. 1.03, CEN/TC 224, Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0059-2009, 2009-12-11

[SSCDT2]

Protection Profile "Secure Signature-Creation Device Type 2", Version: 1.04, EAL 4+, CEN/ISSS, Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0006-2002T (Common Criteria version 2.1 evaluation), 2001-07-25

[TCOSADM]

Administrator's Guidance TCOS Signature Module Version 1.0 Release 1, T-Systems International GmbH Version 1.01, 2011-07-07