Specification of the Security Target TCOS Identity Card Version 1.1 Release 2/P60D144

Version: 1.1.2/20160218

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS Identity Card 1.1.2 (NXP).docx
Stand:	18.02.2016
Version:	1.1.2
Hardware Basis:	P60D144
Autor:	Ernst-G. Giessmann, Markus Blick
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.1.2	2016-02-18	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 Identity Card Version 1.1 Release 2

TOE:	TCOS Identity Card Version 1.1 Release 2/P60D144
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, Markus Blick
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4 augmented.
General Status:	Final
Version Number:	1.1.2
Date:	2016-02-18
Certification ID:	BSI-DSZ-CC-0817-V2
Keywords:	Electronic Identity Card, ID_Card, ePassport, eID, eSign, MRTD, PACE, EAC

3 The TCOS ID-Cards are smart cards with the operating system TCOS. The Identity Card Version 1.0 was based on a different hardware and is conformant to an former version of the Protection Profile [IDCARDPP]. The new hardware and the updates of the Protection Profile are considerd in this Version 1.1 of the TCOS Identity Card.

1.2 TOE Reference

4 The Security Target refers to the Product “TCOS Identity Card Version 1.1 Release 2” (TOE), constisting of configuration ‘01’ and ‘02’ of T-Systems for CC evaluation.

1.3 TOE Overview

5 The Target of Evaluation (TOE) addressed by the current Security Target is the electronic Identity Card (ID_Card) representing a contactless smart card programmed according to the Technical Guideline TR-03110, Version 2.02[1] [EACTR].

[1] Note that the TOE fulfils the stronger requirements of the version 2.10 of the Technical Guideline TR-03110, whereas the Protection Profile is based on the version 2.02 only.

6 For CC evaluation the following applications of corresponding product will be considered[2]:

the Passport Application (*ePassport*) containing the related user data (incl. biometric data) as well as the data needed for authentication (incl. MRZ) as specified in [EACTR, 3.1.1].; with this application the TOE is intended to be used as a machine readable travel document (MRTD);

the *eID*-Application as specified in [EACTR, 3.1.2] including the related user data and the data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application;

the *eSign* Application as specified in [EACTR, 3.1.3] containing data needed for generating advanced or qualified electronic signatures on behalf of the ID_Card Holder as well as for user authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified electronic signature of the ID_Card Holder is required. The eSign application is optional: it means that it can optionally be activated on the ID_Card by a Certification Service Provider Issuer (or on his behalf) authorized by the ID_Card Issuer. It can be set to “operational” or “non-operational” by the ID_Card Holder.

7 The ePassport Application as well as the eID-Application must be accessed through the contact-less interface of the TOE according to [EACTR]. For the eSign Application the interface is not specified in the SSCD PP ([SSCDPP]) and it is out of scope of the Technical Guideline TR-03110 (cf. [EACTR, B.7]).

8 For the ePassport application, the ID_Card Holder can control the access to his user data by conscious presenting his ID_Card to the authorities (CAN or MRZ authentication as specified in [EACTR, 3.3]).

9 For the eID-application, the ID_Card Holder can control the access to his user data by inputting his secret PIN (eID-PIN) or by conscious presenting his ID_Card to the authorities (eID-PIN or CAN user authentication as specified in [EACTR, 3.3].

10 For the eSign application, the ID_Card Holder can control the access to the digital signature functionality by conscious presenting his ID_Card to a Service Provider and using his secret Verification Authentication Data (eSign-PIN, i.e. eSign-VAD as specified in [SSCDPP, 3.2.3.5]).

11 *Application Note 1*: Using a secret PIN represents a manifestation of declaration of intent bound to this secret PIN. In order to reflect this fact, the eID-and the eSign applications shall organzationally get different values of the respective secret PINs (eID-PIN and eSign-PIN). It is especially important, if qualified electronic signatures shall be generated by the eSign application. For security reasons this will not be enforced by the TOE.

[2] The ID_Card support also e.g. the Restricted Identification (RI) described in [EACTR]. Because this functionality is outside the scope of the Protection Profile ([IDCARDPP, p.25]) it is not described here and not part of the evaluation.

12 The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure. The security parameters of these algorithms must be selected by the ID_Card_Issuer according to the Organisational Security Policies [IDCARDPP]. The TOE supports standardized domain parameters mentioned in [RFC5639] (key length 224, 256, 320, 384, 512 bit) and the NIST P-256 curve (key length 256 bit) mentioned in [EACTR, part 3 Table 4].

13 The ID_Card is integrated into a plastic, optically readable part of the Identity Card, This is not part of the TOE.

14 In some context the hardware base may be relevant, and, if so, the TOE will be identified in more detail as the "TCOS Identity Card Version 1.1 Release 1/P60D144PVA", otherwise the notion "TCOS Identity Card Version 1.1 Release 2" will be used, indicating that this context applies to any realization regardless which hardware base is used. Note that the hardware base is identified as P60D144PVA, but this ST may be applied to the P60D080PVA derivate of the same chip too, as it differs only in the memory layout.

15 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]).

16 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

17 The TOE comprises of

- the circuitry of the contactless 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 ePassport, the eID-and, optionally[3] the eSign applications and
- the associated guidance documentation

18 The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated files for the ePassport, the eID-and the eSign application in a file system. A detailed description of the parts of TOE will be given in other documents.

19 Since contactless interface parts (e.g. antenna) may have impact on specific aspects of vulnerability assessment and, thus, be security relevant, these parts are considered in this ST as part of the TOE. The decision upon this was made by the certification body in charge. Further details are considered in the ALC documentation.

[3] activated or not yet activated on the ID_Card

20 The TOE provides two configurations: configuration ‘01’ and configuration ‘02’. Both configurations consist of identical operating system code. The only difference is the TOE identification which can be read out during Personalization Phase by the Personalization Agent (described in the Administrator Guidance [TCOSADM] Annex D). These configurations are only needed to differentiate between two used hardware configurations of [HWCR]. There are no differences in security or funcionality aspects between these configurations.

1.4.2 TOE security features for operational use

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

- Only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the ID_Card under control of the ID_Card holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the service provider connected,
- Creation of digital signatures, if the eSign application is operational,
- Averting of inconspicuous tracing of the ID_Card,
- Self-protection of the TOE security functionality and the data stored inside.

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 terminal (card reader) supporting the contactless communication according to [ISO14443].

23 From the logical point of view, the TOE is able to distinguish between the following terminal types, which, hence, shall be available (see [EACTR], sec. 3.2):

Inspection system: an official terminal that is always operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier),

Authentication terminal: a terminal that may be operated by a governmental organization (Official Domestic Document Verifier) or by any other organization (Non-Official / Foreign Document Verifier), and

Signature terminal: a terminal used by ID_Card holder for generation of digital signatures.

24 The TOE requires terminal of each type to authenticate itself before access according to effective terminal authorization is granted. To authenticate a terminal either as an in-

spection system or authentication terminal or signature terminal, General Authentication Procedure[4] must be used.

25 The TOE will not support Basic Access Control (BAC), see [EACTR], sec. 1.1, 3.1.1 and Appendix G, because the file system of the TOE does not contain the BAC keys after Initialization and the security features of the TOE do not allow to create them later on.

26 The authorization level of an authenticated terminal shall be determined by the effective terminal authorization calculated from the certificate chain presented by this terminal to the TOE. All necessary certificates of the related public key infrastructure – Country Verifying Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Terminal Certificates – shall be available in a card verifiable format as specified in [EACTR, Appendix C.1 and sec. 2.2.3.].

27 The following table gives an overview which types of terminals shall be supported for which single application of the TOE, see [11], sec. 3.1 – 3.4 (please note that the effective ability of a terminal depends on its terminal authorization level finally derived from the presented certificate chain as stated above):

	Inspection System (official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
ePassport	Operations: reading all Data Groups User Authentication: CAN, MRZ for PACE In this context the terminal is equivalent to an EIS [EACPP3.1]	No operations	No Operations
eID	Operations: reading all Data Groups User Authentication: CAN for PACE	Operations: writing a subset of Data Groups, reading all or a subset of Data Groups User Authentication: eID-PIN, eID-PUK or CAN for PACE	No Operations
eSign	No Operations	Operations: activating eSign application User Authentication: eID-PIN, eID-PUK or CAN for PACE In this context the terminal is equivalent the CGA in [SSCDPP] and	Operations: generating digital signatures User Authentication: CAN for PACE followed by eSign-PIN through the HID In this context the terminal is equivalent to the SGA in [SSCDPP] and

[4] i.e. executing the protocol sequence PACE, Terminal Authentication, Passive Authentication and Chip Authentication according to [EACTR,part 2 sec. 3.2, 3.3 and 3.4]

		implements the corresponding HID.	may implement the corresponding HID

1.4.4 Life Cycle Phases Mapping

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

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

29 According to the PP [IDCARDPP] the TOE life cycle is described in terms of the four life cycle phases.

Life cycle phase 1 “Development”

30 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.

31 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.

32 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 eID_Card application and the guidance documentation is securely delivered to the eID_Card manufacturer.

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

Life cycle phase 2 “Manufacturing”

34 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 eID_Card material during the IC manufacturing and the delivery process to the eID_Card manufacturer. The IC is securely delivered from the IC manufacturer to the eID_Card manufacturer (note that both of these roles may be assigned to different entities).

35 The inlay holding the chip as well as the antenna and the plastic with optical readable part, (holding the e.g. the printed MRZ) are necessary to represent a complete Identity Card, nevertheless they are not inevitable for the secure operation of the TOE.

36 The eID_Card manufacturer

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

(ii) creates the ePassport, the eID-and the eSign application, and

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

(iv) packs the IC with hardware for the contactless interface in the eID_Card.

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

38 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 issuing states or organizations. The mentioned restrictions 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.

39 The eSign 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 eSign application. Based on the Administrator Guidance [TCOSADM] the activating CSP develops a corresponding User Guidance for the eSign Application, which is delivered to the eID_Card holder by the CSP. Note that the TOE has no contact interface. The eSign Application can be used through the contactless interface only.

40 For the TOE two pre-configured versions ('01' and '02') of the system apply. A detailed description of the sub-phases and the system pre-configurations, including the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSADM].

41 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]. Note that the physical interface (i.e. the antenna) is out of the scope of the PP0035. Therefore it is not considered in the life cycle phases mapping.

Life cycle phase 3 "Issuing"

42 The personalization of the eID_Card includes

(i) the survey of the eID_Card holder biographical data,

(ii) the enrolment of the eID_Card holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),

(iii) the printing of the visual readable data onto the plastic cover of the physical eID_Card,

(iv) the writing of TOE User Data and TSF Data into the logical eID_Card and

(v) configuration of the TSF if necessary (not applicable for the TOE).

43 The step (iv) is performed by the Personalization Agent.

44 The personalized eID_Card (together with appropriate guidance for TOE use if necessary) is handed over to the eID_Card holder for operational use.

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

46 *Application Note 2*: 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”

47 The TOE is used as eID_Card’s chip by the eID_Card holder and the terminals in the “Operational Use” phase.

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

49 If the eSign application is not activated during Personalization, and only an authorized terminal (the User S.Admin according [SSCDPP]) can execute the eSign key pair generation. The qualified certificate will be assigned to the ID_Card holder identified by the authorized terminal. Therefore no further Personalization procedure is required in Phase 7 (Operational Use).

50 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

51 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.

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

53 The physical constituents of the TOE are the operating system, the data in elementary files of the dedicated files of the ePassport, eID and the eSign application (EEPROM),

and temporary data used during execution of procedures associated to that dedicated file.

1.4.5.2 TOE Logical Boundaries

54 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.

55 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).

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

57 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

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

Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, Sept. 2012,

Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, Sept. 2012,

Part 3: Security Assurance Requirements; CCMB-2012-09-00, Version 3.1, Revision 4, Sept. 2012

59 as follows:

Part 2 extended,

Part 3 conformant.

60 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012, [CC] has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

2.2 PP Claims

61 This ST claims strict conformance to the CC Protection Profile Electronic Identity Card (ID_Card PP), Version 1.03, BSI-PP-0061, 2009-12-15 [IDCARDPP].

62 As required by the CC Protection Profile Electronic Identity Card (ID_Card PP) the strict conformance to this PP includes the strict conformance to the CC Protection Profile Secure Signature Creation Device – Part 2: Device with key generation, Version 1.03, BSI-PP-0059 [SSCDPP]. Therefore the Security Requirements of the latter will be considered in this ST too.

2.3 Package Claims

63 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.

64 The evaluation assurance level of the TOE is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in [CC].

2.4 Conformance Rationale

65 The ST claims *strict* conformance to the protection profile SSCD Core PP [SSCDPP] as required there in sec. 6.4. The part of the security policy for the ePassport application of

the TOE is contextually in a tight connection with the ICAO EAC PP [EACPP3.1]. Due to this fact, it is sensible to distinguish between separated sets of {TOE type, SPD statement, security objectives statement, security requirements statement} for each application residing in the TOE: ePassport, eID-and eSign, respectively, unless the items are identical or hierarchical as in the case of the SARs.

66 The **TOE type** stated in [SSCDPP], sec. 5.4.2 is '… a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory'.

67 This TOE type is obviously commensurate with the current TOE type in the part being provided by the eSign application as stated above.

68 The **Security Problem Definition** (SPD) of the PP ([IDCARDPP]) contains the security problem definition of the PP [SSCDPP]. The current SPD includes the same threats, organizational security policies and assumptions as for the TOE in [SSCDPP] and comprehends several additional items as stated in chap. 3 below.

69 Strict conformance presumes that assumptions of the PP ([IDCARDPP]) shall be identical to the assumptions of each PP to which the conformance is being claimed. In this context, the current assumptions block for the eSign application is identical to the assumptions from [SSCDPP].

70 The **Security Objectives Statement** for the TOE in the PP ([IDCARDPP]) includes all the security objectives for the TOE of the PP [SSCDPP] and comprehends several additional items as stated in chap. 4.1 below. The Security Objectives Statement for the TOE's operational environment in the PP ([IDCARDPP]) includes all security objectives for the operational environment of the PP [SSCDPP] and comprehends several additional items as stated in chap. 4.2 below. In this context, the current block of environmental objectives for the eSign application is identical to the equivalent objectives from [SSCDPP].

71 The **Security Requirements Statement** for the TOE in the current ST includes all the SFRs for the TOE of the PP [SSCDPP] and comprehends several additional items as stated in chap. 6.1 below. The SAR statement for the TOE in the current ST includes all the SARs for the TOE of the PP [SSCDPP] as stated in chap. 6.2 below. The current assurance package contains the assurance component ALC_DVS.2 and ATE_DPT.2 being hierarchical to ALC_DVS.1 and ATE_DPT.1 as required by [SSCDPP]. Strict conformance allows that the security requirements for the TOE may be hierarchically stronger than those items of each PP to which the conformance is being claimed.

3 Security Problem Definition

72 The ST covers three different applications – ePassport, eID- and eSign –, therefore the SPD statement of the TOE, as well as the Security Objectives and the Security Requirements for the TOE in the following chapters are traced to the corresponding applications.

3.1 Introduction

Assets

73 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
ePassport, eID, eSign			
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the applications of the ID_Card as defined in [EACTR] and (i) being allowed to be *read out* or *written* solely by an authenticated terminal (in the sense of [EACTR], sec. 3.2) respectively (ii) being allowed to be *used* solely by an authenticated terminal (in the sense of [EACTR], sec. 3.2) (the private Restricted Identification key[5]) respectively (iii) being allowed to be *used* solely by the authenticated ID_Card holder (the private signature key within the eSign application). This asset covers 'User Data on the MRTD's chip' and 'Logical MRTD_Card sensitive User Data' in [EACPP3.1] as well as 'SCD' and 'DTBS-representation' in [SSCDPP].	Confidentiality[6] Integrity Authenticity
2	user data transferred between the TOE and the service provider connected[7]	All data (being not authentication data) being transferred in the context of the applications of the ID_Card as defined in [EACPP3.1] between the TOE and an authenticated terminal (in the sense of [EACPP3.1, sec. 3.2]. User data can be received and sent. This asset covers 'DTBS' in [SSCDPP].	Confidentiality[6] Integrity Authenticity
3	ID_Card tracing data	Technical information about the current and previous locations of the ID_Card gathered by inconspicuous (for the ID_Card holder) recognizing	Unavailability[8]

[5] Since the Restricted Identification according to [EACTR, part 2 sec. 3.5] represents just a functionality of the ID_Card, the key material needed for this functionality and stored in the TOE is treated here as User Data in the sense of the CC.

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

[7] For the ePassport application, the service provider is always an authority represented by a local RF-terminal

[8] represents a prerequisite for anonymity of the ID_Card holder

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
		the TOE knowing *neither* CAN *nor* MRZ *nor* eID-PIN *nor* eID-PUK. TOE tracing data can be provided / gathered.	

Table 1: Primary assets

74 *Application Note 3*: Please note that user data being referred in the table above include, amongst other, individual-related (personal) data of the ID_Card holder which also include his sensitive (biometrical) data. Hence, the general security policy defined by the PP [IDCARDPP] also secures these specific ID_Card holder's data as specified in the table above.

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

76 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
ePassport, eID, eSign			
4	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
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [EACPP3.1].	Availability
6	TOE immanent secret cryptographic keys	Secret cryptographic material used by the TOE in order to enforce its security functionality[9].	Confidentiality Integrity
7	TOE immanent non-secret cryptographic keys	Non-secret cryptographic material used by the TOE in order to enforce its security functionality. This asset covers 'SVD' in [SSCDPP].	Integrity Authenticity
8	Secret ID_Card holder authentication data	Secret authentication information for the ID_Card holder being used for verification of the authentication attempts as authorized ID_Card holder: • eID-PIN and eID-PUK stored in the ID_Card as well as • eSign-PIN (and eSign-PUK, if any[10]) (i) stored in the ID_Card[11] and (ii) transferred to it[12]	Confidentiality Integrity

[9] please note that the private signature key within the eSign application (SCD) belongs to the object No. 1 'user data stored' above.

[10] eSign-PIN and eSign-PUK are local secrets being valid only within the eSign application

[11] is commensurate with RAD in [SSCDPP]

[12] is commensurate with VAD in [SSCDPP]

Object No.	Asset	Definition	Property to be maintained by the current security policy
9	ID_Card communication establishment authorization data	Restricted-revealable[13] authorization information for a human user being used for verification of the authorization attempts as authorized user (CAN for ePassport, eID, eSign; MRZ for ePassport). These data are stored in the TOE and are not to convey to it.	Confidentiality[13] Integrity

Table 2: Secondary assets

77 *Application Note 4*: ID_Card holder authentication and ID_Card communication establishment authorization data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authentication/authorization attempt. The TOE shall secure the reference information as well as — together with the terminal connected[14] — the verification information in the TOE–Terminal channel, if it has to be transferred to the TOE. Please note that CAN, MRZ, eID-PIN and eID-PUK are not to convey to the TOE.

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

Subjects and external entities

79 This ST considers the following subjects:

External Entity	Subject	Role	Definition
1	1	ID_Card holder	A person for whom the ID_Card Issuer has personalized the ID_Card[15]. This subject is commensurate with ‘MRTD_Card Holder’ in [EACPP3.1] and ‘S.Signatory’ in [SSCDPP]. Please note that an ID_Card holder can also be an attacker (s. below).
2	–	ID_Card presenter	A person presenting the ID_Card to a terminal[16] and claiming the identity of the ID_Card holder. This subject is commensurate with ‘Traveller’ in [EACPP3.1] and ‘S.User’ in [SSCDPP]. Please note that an ID_Card holder can also be an attacker (s. below).
3	–	Service Provider (SP)	An official or commercial organization providing services which can be used by the ID_Card holder. Service Provider uses the rightful terminals managed by a DV.
4	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role ‘Terminal’ is the default role for any terminal being recognized by the TOE as neither PCT nor EIS nor ATT nor SGT (‘Terminal’ is used by the ID_Card presenter). This subject is commensurate with ‘Terminal’ in [EACPP3.1]
5	3	PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the ID_Card and the related value presented to the terminal by the ID_Card presenter.

[13] The ID_Card holder may reveal, if necessary, verification values of the CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.

[14] the input device of the terminal

[15] i.e. this person is uniquely associated with a concrete electronic ID Card

[16] in the sense of [EACTR]

External Entity	Subject	Role	Definition
			PCT implements the terminal's part of the PACE protocol and authenticates itself to the ID_Card using a shared password (CAN, eID-PIN, eID-PUK or MRZ). The PCT is not allowed reading User Data (see sec. 4.2.2 in [EACTR]). See also [EACTR, chap. 3.3, 4.2, table 1.2 and G.2]
6	4	Inspection system (EIS)	A technical system being used by an authority[17] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ID_Card presenter as the ID_Card holder (for *ePassport*: by comparing the real biometrical data of the ID_Card presenter with the stored biometrical data of the ID_Card holder). An Inspection System is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorized by the ID_Card Issuer through the Document Verifier of the receiving State (by issuing terminal certificates) to read a subset of the data stored on the ID_Card. The Inspection System in the context of [EACTR] and of [IDCARDPP]) is commensurate with the Extended Inspection System (EIS) as defined in [EACPP3.1]. See also [EACTR, chap. 3.2 and C.4].
7	5	Authentication Terminal (ATT)	A technical system being operated and used either by a governmental organization (Official Domestic Document Verifier) or by any other, also commercial organization and (i) verifying the ID_Card presenter as the ID_Card holder (using the secret eID-PIN[18]), (ii) updating a subset of data of the eID-application and (iii) installing the eSign application. An Authentication Terminal is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorized by the ID_Card Issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset of the data stored on the ID_Card. See also [EACTR, chap. 3.2 and C.4].
8	6	Signature Terminal (SGT)	A technical system being approved by a Certification Service Provider and used for generation of digital signatures. A Signature Terminal is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorized by the ID_Card Issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset of the data stored on the ID_Card. See also [EACTR, chap. 3.2 and C.4].
9	7	Document Verifier (DV)	An organization enforcing the policies of the CVCA and of a Service Provider (governmental or commercial organization) and managing the terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [EACTR], chap. 2.2.2. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ID_Card Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement[19] between the ID_Card Issuer und a foreign CVCA ensuring enforcing the ID_Card Issuer's privacy policy[20]). This subject is commensurate with 'Document Verifier' in [EACPP3.1].

[17] concretely, by a control officer

[18] the secret eID-PUK can be used for unblocking the eID-PIN and resetting the retry counter related.

[19] the form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the [IDCARDPP] in order to reflect an appropriate relationship between the parties involved.

[20] Existing of such an agreement may technically be reflected by means of issuing a C_{CVCA-F} for the Public Key of the foreign CVCA signed by the domestic CVCA.

External Entity	Subject	Role	Definition
10	8	Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the ID_Card Issuer with respect to protection of user data stored in the ID_Card (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the rightful terminals (EIS, ATT, SGT) and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EACTR], chap. 2.2.1. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [EACTR]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EACTR], sec. 2.2.1. This subject is commensurate with ‘Country Verifying Certification Authority’ in [EACPP3.1].
11	–	Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Card Security Object stored on the ID_Card for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR]. This role is usually delegated to a Personalization Agent.
12	–	Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the ID_Card Issuer with respect to confirming correctness of user and TSF data stored in the ID_Card. The CSCA represents the country specific root of the PKI for the ID_Cards and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [EACTR], 5.1.1. The Country Signing CertA issuing certificates for Document Signers (cf. [EACTR]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EACTR], sec. 2.2.1.
13	–	Certification Service Provider (CSP)	An organization issuing certificates and providing other services related to electronic signatures. There can be Common and Qualified CSP: A Qualified Certification Service Provider issues qualified certificates. A CSP is the Certification Service Provider in the sense of [SSCDPP]. This subject is commensurate with ‘S.Admin’ in [SSCDPP].
14	9	Personalization Agent	An organization acting on behalf of the ID_Card Issuer to personalize the ID_Card for the ID_Card holder by some or all of the following activities: (i) establishing the identity of the ID_Card holder for the biographic data in the ID_Card[21], (ii) enrolling the biometric reference data of the ID_Card holder[22], (iii) writing a subset of these data on the physical Identification Card (optical personalization) and storing them in the ID_Card (electronic personalization) for the ID_Card holder as defined in EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card Security Object defined in [EACTR] (in the role of DS). Please note that the role ‘Personalization Agent’ may be distributed among several institutions according to the operational policy of the ID_Card 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].
15	10	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the ID_Card Manufacturer completing the IC to the ID_Card. 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 ID_Card Manufacturer using this role Manufacturer. This subject is commensurate with ‘Manufacturer’ in [EACPP3.1].
16	11	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

[21] relevant for the ePassport, the eID and the eSign applications

[22] relevant for the ePassport application

External Entity	Subject	Role	Definition
			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 including the entities mentioned in footnote 13 on page 18 to which the CAN or MRZ may be revealed. This subject is commensurate with 'Attacker' in [EACPP3.1] and 'S.Offcard' in [SSCDPP].

Table 3: Subjects

80 Since the file system of the TOE does not support BAC, the Basic Inspection System (BIS) cannot be recognized by the TOE, see above.

3.2 Threats

81 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.

82 The following threats are defined in the current ST (they are derived from the ICAO-BAC PP [BACPP3.1] and ICAO-EAC PP [EACPP3.1]):

T.Skimming **Skimming ID_Card/Capturing Card–Terminal Communication**

83 An attacker imitates an inspection system, an authentication or a signature terminal in order to get access to the user data stored on or transferred between the TOE and the service provider connected via the contactless interface of the TOE. The attacker cannot read and does not know the correct value of the shared password (CAN, MRZ, eID-PIN, eID-PUK or MRZ) in advance.
This item concerns the following application(s): ePassport, eID, eSign.

84 *Application Note 5*: This threat also covers the item T.Read_Sensitive_Data in the ICAO-EAC PP [EACPP3.1]: Sensitive biometric reference data stored on the ID_Card are part of the asset *user data stored on the TOE*. Knowledge of the Document Basic Access Keys is here not applicable, because the TOE does not support the BAC protocol and, therefore, the Document Basic Access Keys are not existent for the TOE.

85 *Application Note 6*: MRZ is printed and CAN is printed or stuck on the Identification Card. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.ID_Card-Holder.

T.Eavesdropping **Eavesdropping on the communication between the TOE and a rightful terminal**

86 An attacker is listening to the communication between the ID_Card and a rightful terminal in order to gain the *user data transferred between the TOE and the service provider connected*.
This item concerns the following application(s): ePassport, eID, eSign.

87 *Application Note 7*: A product supporting BAC cannot avert this threat in the context of the security policy defined in the [IDCARDPP].

T.ID_CARD_Tracing Tracing ID_Card

88 An attacker tries to gather TOE tracing data (i.e. to trace the movement of the ID_Card) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE. The attacker cannot read and does not know the correct values of shared passwords (CAN, MRZ, eID-PIN, eID-PUK) in advance.
This item concerns the following application(s): ePassport, eID, eSign.

89 *Application Note 8*: A product supporting BAC cannot avert this threat in the context of the security policy defined in the [IDCARDPP].

T.Forgery Forgery of Data

90 An attacker fraudulently alters the User Data or/and TSF-data stored on the ID_Card or/and exchanged between the TOE and the Service Provider connected in order to outsmart the authenticated terminal (EIS, ATT or SGT) by means of the changed ID_Card holder’s related reference data (like biographic or biometric data or SCD/SVD). The attacker does it in such a way that the Service Provider (represented by the terminal connected) perceives these modified data as authentic one.
This item concerns the following application(s): ePassport, eID, eSign.
This threat partially covers T.SVD_Forgery (only stored, but not being sent to the CGA SVD) from [SSCDPP].

T.Counterfeit Counterfeiting ID_Card

91 An attacker produces an unauthorized copy or reproduction of a genuine ID_Card to be used as part of a counterfeit Identification Card: He may generate a new data set or extract completely or partially the data from a genuine ID_Card and copy them on another functionally appropriate chip to imitate this genuine ID_Card. This violates the authenticity of the ID_Card being used either for authentication of an ID_Card presenter as the ID_Card holder or for authentication of the ID_Card as a genuine secure signature creation device.
This item concerns the following application(s): ePassport, eID, eSign.

T.Abuse-Func Abuse of Functionality

92 An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclosure the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and the personalization in the operational phase after delivery to the ID_Card holder.
This item concerns the following application(s): ePassport, eID, eSign.
This threat covers T.SigF_Misuse from [SSCDPP].

93 *Application Note 9*: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage Information Leakage from ID_Card

94 An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data. The information leakage may be

inherent in the normal operation or caused by the attacker.
This item concerns the following application(s): ePassport, eID, eSign.

95 *Application Note 10*: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper Physical Tampering

96 An attacker may perform physical probing of the ID_Card in order

(i) to disclose the TSF-data, or

(ii) to disclose/reconstruct the TOE's Embedded Software.

97 An attacker may physically modify the ID_Card in order to modify

(i) its security functionality (hardware and software part, as well),

(ii) the User Data or the TSF-data stored on the ID_Card.

98 This item concerns the following application(s): ePassport, eID, eSign.

99 This threat covers T.Hack_Phys from [SSCDPP].

100 *Application Note 11*: The physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the ID_Card) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the ID_Card's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction Malfunction due to Environmental Stress

101 An attacker may cause a malfunction the ID_Card's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the ID_Card outside the normal operating conditions, exploiting errors in the ID_Card's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.
This item concerns the following application(s): ePassport, eID, eSign.

102 *Application Note 12:* A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation

(refer to the threat T.Phys-Tamper) assuming a detailed knowledge about the TOE's internals.

103 The PP ([IDCARDPP]) also includes all threats of the SSCD PP [SSCDPP]. If the *eSign* application is operational then all these items are applicable. For the sake of completeness the threats are listed below. More details can be found in the SSCD PP [SSCDPP].

Threat identifier	Comments
T.SCD_Divulge	concerns the following application(s): – eSign
T.SCD_Derive	concerns the following application(s): – eSign
T.Hack_Phys is covered by T.Phys-Tamper	concerns the following application(s): – ePassport – eID – eSign
T.SVD_Forgery is covered by T.Forgery	concerns the following application(s): – eSign
T.SigF_Misuse is covered by T.Abuse-Func	concerns the following application(s): – ePassport – eID – eSign
T.DTBS_Forgery	concerns the following application(s): – eSign
T.Sig_Forgery	concerns the following application(s): – eSign

3.3 Organizational Security Policies

104 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.Pre-Operational Pre-operational handling of the ID_Card

1. The ID_Card Issuer issues ID_Cards and approves terminals complying with all applicable laws and regulations.
2. The ID_Card Issuer guarantees the correctness of the user data (amongst other of those, concerning the ID_Card holder) and of the TSF-data permanently stored in the TOE[23].
3. The ID_Card Issuer uses only such TOE's technical components (IC) which enable traceability of the ID_Cards in their manufacturing and issuing life phases, i.e. *before* they are in the operational phase.
4. If the ID_Card Issuer authorizes a Personalization Agent to personalize the ID_Card for the ID_Card holder, the ID_Card Issuer has to ensure that the Personalization Agent acts in accordance with the ID_Card Issuer's policy.

[23] cf. Table 1 and Table 2 above

105 This item concerns the following application(s): ePassport, eID, eSign.

P.ID_Card_PKI PKI for Chip and Passive Authentication[24] (issuing branch)

106 *Application Note 13*: 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 ID_Card Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the ID_Card. For this aim he runs a Country Signing Certification Authority (CSCA). The ID_Card Issuer shall distribute the Country Signing CertA Certificate (CCSCA) and the Document Signer Certificates (CDS) to the CVCA (who forwards them finally to the rightful terminals).
2. The CSCA shall securely generate, store and use the Country Signing CertA Key pair. The CSCA shall keep the Country Signing CertA Private Key secret and issue a self-signed Country Signing CertA Certificate (CCSCA) having to be distributed to the ID_Card Issuer by strictly secure means, see [ICAO9303-1], 5.1.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and distribute them to the ID_Card Issuer, see [ICAO9303-1, 5.1.1].
3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret, (iv) securely use the Document Signer Private Key for signing the Card Security Objects of the ID_Cards and (v) manage the Chip Authentication Key Pairs {SKPICC, PKPICC} used for the chip authentication as defined in [EACTR], sec. 4.3.

107 This item concerns the following application(s): ePassport, eID, eSign.

P.Terminal_PKI PKI for Terminal Authentication (receiving branch)

108 *Application Note 14*: 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 ID_Card Issuer shall establish a public key infrastructure for the card verifiable certificates used for terminal authentication. For this aim, the ID_Card Issuer shall run a domestic Country Verifying Certification Authority (domestic CVCA) and may use already existing foreign CVCAs[25]. The ID_Card Issuer shall make the CVCA Link Certificate available to the CSCA (who shall finally distribute it to its ID_Cards).
2. A CVCA shall securely generate, store and use the CVCA key pair. A CVCA shall securely generate, store and use the CVCA key pair. A CVCA shall keep the CVCA

[24] Passive authentication is considered to be part of the Chip Authentication protocol.

[25] 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.

Private Key secret and issue a self-signed CVCA Certificate (C_{CVCA}) having to be made available to the ID_Card Issuer by strictly secure means as well as to the respective Document Verifiers. A CVCA shall create the Document Verifier Certificates for the Document Verifier Public Keys (C_{DV}) and distribute them back to the respective Document Verifier Verifiers[26].

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)[27].
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.

109 This item concerns the following application(s): ePassport, eID, eSign.

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 ID_Cards.
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)[28].
3. CSPs shall ensure that they issue their certificates exclusively for the rightful data (public signature key of the ID_Card holder)[29].

110 This item concerns the following application(s): ePassport, eID, eSign.

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 ID_Card holders as defined in [EACTR], sec. 3.2.
2. They shall implement and use the terminal parts of the PACE protocol [EACTR, part 2 sec. 3.2], of the Terminal Authentication protocol [EACTR, part 2 sec. 3.4], of the Passive Authentication [EACTR, part 1 sec. 1.1] and of the Chip Authentication protocol [EACTR, part 2 sec. 3.3][30] and use them in this order[31]. A rightful terminal

[26] A CVCA shall also manage a Revocation Sector Key Pair {$SK_{Revocation}$, $PK_{Revocation}$} [EACTR, part 2 sec.3.5].

[27] A DV shall also manage a Revocation Sector Key Pair {$SK_{SectorNN}$, $PK_{SectorNN}$} [EACTR,part 2 sec. 3.5].

[28] This rule is relevant for T.Skimming

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

[30] The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within [IDCARDPP]

shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

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 ID_Card) 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. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the Chip Authentication after the Terminal Authentication[32].
6. A rightful terminal and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PINs/PUKs, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

111 This item concerns the following application(s): ePassport, eID, eSign.

112 The PP ([IDCARDPP]) also includes all OSPs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

113 For the sake of completeness the OSPs are listed below. More details can be found in the SSCD PP [SSCDPP].

OSP identifier	Comments
P.CSP_QCert	concerns the following application(s): – eSign
P.QSign	concerns the following application(s): – eSign
P.Sigy_SSCD	concerns the following application(s): – eSign
P.Sig_Non-Repud	concerns the following application(s): – eSign

Table 4: OSPs taken over from [SSCDPP]

[31] This order is only commensurate with the General authentication Procedure decribed in section 2.4 of [EACTR, part 2]. Other branches of this figure are not covered by the security policy of [IDCARDPP].

[32] This rule is relevant for T.Skimming

3.4 Assumptions

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

115 The current ST includes all assumptions of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

116 For the sake of completeness the assumptions are listed below. More details can be found in the SSCD PP [SSCDPP].

Assumption identifier	Comments
A.CGA	concerns the following application(s): – eSign
A.SCA	concerns the following application(s): – eSign

Table 5: Assumptions taken over from [SSCDPP]

117 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 7.10.2 of the current ST.

118 The PP ([IDCARDPP]) does not include any additional assumptions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.Data_Integrity Integrity of Data

121 The TOE must ensure integrity of the User Data and the TSF-data[33] stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying).
The TOE must ensure integrity of the User Data and the TSF-data[33] during their exchange between the TOE and the Service Provider connected (and represented by either EIS or ATT or SGT) after the Terminal- and the Chip Authentication.
This item concerns the following application(s): ePassport, eID, eSign.

OT.Data_Authenticity Authenticity of Data

122 The TOE must ensure authenticity of the User Data and the TSF-data[34] stored on it by enabling verification of their authenticity at the terminal-side[35].
The TOE must ensure authenticity of the User Data and the TSF-data[34] during their exchange between the TOE and the Service Provider connected (and represented be either EIS or ATT or SGT) after the Terminal and the Chip Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[36].
This item concerns the following application(s): ePassport, eID, eSign.

OT.Data_Confidentiality Confidentiality of Data

123 The TOE must ensure the confidentiality of the User Data and the TSF-data[37] by granting read access only to authorized rightful terminal (EIS, ATT, SGT) according to the terminal authorization level (CHAT) presented by the terminal connected.
The TOE must ensure the confidentiality of the User Data and the TSF-data[37] during their exchange between the TOE and the Service Provider connected (and represented be either EIS or ATT or SGT) after the Terminal- and the Chip Authentication.
This item concerns the following application(s): ePassport, eID, eSign.

[33] where appropriate, see Table 2 above

[34] where appropriate, see Table 2 above

[35] verification of SO_C

[36] Secure messaging after the chip authentication, see also [EACTR, part 2 sec. 3.3.2

[37] where appropriate, see Table 2 above

OT.ID_Card_Tracing Tracing ID_Card

124 The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the ID_Card remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared passwords (CAN, MRZ, eID-PIN, eID-PUK) in advance.
This item concerns the following application(s): ePassport, eID, eSign.

OT.Chip_Auth_Proof Proof of ID_Card authenticity

125 The TOE must enable the terminal connected to verify the authenticity of the ID_Card as a whole device as issued by the ID_Card Issuer (issuing PKI branch of the ID_Card Issuer) by means of Passive and Chip Authentication as defined in [EACTR, part 2 sec. 3.3].
This item concerns the following application(s): ePassport, eID, eSign.

126 *Application Note 15:* The OT.Chip_Auth_Proof implies the ID_Card's chip to have a secret to prove its authenticity by knowledge, i.e. a Chip Authentication Private Key as TSF-data.
The terminal shall have the reference data to verify the authentication attempt of ID_Card's chip, i.e. a certificate for the respective Chip Authentication Public Key (PK_{PICC}) fitting to the Chip Authentication Private Key (SK_{PICC}). This certificate is provided by (i) the Chip Authentication Public Key stored on the TOE and (ii) the hash value of this PK_{PICC} in the Card Security Object (SO_C) signed by the Document Signer.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

127 The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.
This item concerns the following application(s): ePassport, eID, eSign.

OT.Prot_Inf_Leak Protection against Information Leakage

128 The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the ID_Card

- by 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 forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE

129 This item concerns the following application(s): ePassport, eID, eSign.

130 *Application Note 16:* This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper Protection against Physical Tampering

131 The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF-data and the ID_Card's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)

with a prior

- reverse-engineering to understand the design and its properties and functionality

132 This item concerns the following application(s): ePassport, eID, eSign.

OT.Prot_Malfunction Protection against Malfunctions

133 The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.
This item concerns the following application(s): ePassport, eID, eSign.

134 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

135 The TOE must provide means to store Initialization[38] 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 ID_Card.
This item concerns the following application(s): ePassport, eID, eSign.

OT.Personalization Personalization of ID_Card

136 The TOE must ensure that the user data (amongst other those concerning the ID_Card holder[39]) 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 optional *eSign* application can additionally be activated on the TOE on behalf of the CSP

[38] amongst other, IC Identification data

[39] biographical and biometrical data as well as the SCD, if the eSign is operational

taking responsibility for this *eSign* application, if the ID_Card holder had applied for this.
This item concerns the following application(s): ePassport, eID, eSign.

137 The PP ([IDCARDPP]) also includes all security objectives for the TOE of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

138 For the sake of completeness the objectives are listed below. More details can be found in the SSCD PP [SSCDPP].

Objective identifier	Comments
OT.Lifecycle_Security	concerns the following application(s): – eSign
OT.SCD/SVD_Gen	concerns the following application(s): – eSign
OT.SCD_Unique	concerns the following application(s): – eSign
OT.SCD_SVD_Corresp	concerns the following application(s): – eSign
OT.SCD_Secrecy	concerns the following application(s): – eSign
OT.Sig_Secure	concerns the following application(s): – eSign
OT.Sigy_SigF	concerns the following application(s): – eSign
OT.DTBS_Integrity_TOE	concerns the following application(s): – eSign
OT.EMS_Design	concerns the following application(s): – eSign
OT.Tamper_ID	concerns the following application(s): – eSign
OT.Tamper_Resistance	concerns the following application(s): – eSign

Table 6: TOE objectives taken over from [SSCDPP]

4.2 Security Objectives for the Operational Environment

I. ID_Card Issuer as the general responsible

139 The ID_Card Issuer as the general responsible for the global security policy related will implement the following security objectives of the TOE environment:

OE.Legislative_Compliance

140 The ID_Card Issuer must issue ID_Cards and approve using the terminals complying with all applicable laws and regulations.
This item concerns the following application(s): ePassport, eID.

II. ID_Card Issuer and CSCA: ID_Card's PKI (issuing) branch

141 The ID_Card Issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Passive_Auth_Sign Authentication of ID_Card by Signature

142 The ID_Card Issuer has to establish the necessary public key infrastructure as follows: The CSCA acting on behalf and according to the policy of the ID_Card Issuer must (i) generate a cryptographic secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) make the Certificate of the CSCA Public Key (C_{CSCA}) and the Document Signer Certificates (C_{DS}) available to the ID_Card Issuer, who makes them available to his own (domestic) CVCA as well as to the foreign CVCAs under agreement[40]. Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographic secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Card Security Objects of genuine ID_Cards in a secure operational environment only. The digital signature in the Card Security Object relates to all security information objects according to [EACTR, part 2 Appendix A].

The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DS must sign exclusively correct Card Security Objects having to be stored on the ID_Cards.

This item concerns the following application(s): ePassport, eID.

This item also covers OE.CGA_SSCD and partially OE.SVD_Auth from Table 7 below for the eSign application.

OE.Chip_Auth_Key Chip Authentication Key

143 A Document Signer acting in accordance with the CSCA policy has to (i) generate the ID_Card's Chip Authentication Key Pair {SK_{PICC}, PK_{PICC}} used for the chip authentication as defined in [EACTR, part 2 sec. 3.3], (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key Info (Appendix A of [EACTR, part 3]) and (iii) support Service Providers to verify the authenticity of the ID_Card's chips used for genuine ID_Cards by certification of the Chip Authentication Public Key by means of the Card Security Object.

A Document Signer has also to manage Restricted Identification Key Pairs {SK_{ID}, PK_{ID}} [EACTR, part 2 sec. 3.5]: the private Restricted Identification Key SK_{ID} is to store in the TOE, whereby the public Restricted Identification Key PK_{ID} – in a database of the DS.

This item concerns the following application(s): ePassport, eID.

This item also covers OE.CGA_SSCD and partially OE.SVD_Auth from Table 7 below for the eSign application.

OE.Personalization Personalization of ID_Card

144 The ID_Card Issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the ID_Card holder and create the biographical data for the ID_Card[41], (ii) enroll the biometric reference data of the ID_Card holder[42], (iii) write a

[40] CVCAs represent the roots of the receiving branch, see below

[41] relevant for the ePassport, the eID and the eSign applications

subset of these data on the physical Identification Card (optical personalization) and store them in the ID_Card (electronic personalization) for the ID_Card holder as defined in [EACTR], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Card Security Object defined in [ICAO9303-1] (in the role of a DS).
This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.CGA_QCert from Table 7 below for the eSign application.

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

145 The ID_Card Issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the ID_Card Issuer Card Issuer)[43] will implement the following security objectives of the TOE environment:

OE.Terminal_Authentication Authentication of rightful terminals

146 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[44]) 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, part 2 sec. 3.5].
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. A DV has also to manage Sector's Static Key Pairs {$SK_{SectorNN}$, $PK_{SectorNN}$} [EACTR, part 2 sec. 3.5].
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, part 2 sec. 3.4] 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)[45].

[42] relevant for the ePassport application

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

[44] CSCA represents the root of the issuing branch, see above.

[45] This rule is relevant for T.Skimming

This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.SVD_Auth from Table 7 below for the eSign application.

OE.Terminal **Terminal operating**

147 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, part 2 sec. 2.2].
2. Their terminals implement and use the terminal parts of the PACE protocol [EACTR, part 2 sec. 3.2], of the Terminal Authentication protocol [EACTR, part 2 sec. 3.4], of the Passive Authentication [EACTR, part 1 sec. 1.1] (by verification of the signature of the Card Security Object) and of the Chip Authentication protocol [EACTR, part 2 sec. 3.3][46] and use them in this order[47]. 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, part 2 sec. 3.4]).
5. Their terminals must not send assets (e.g. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the Chip Authentication after the Terminal Authentication[48].
6. Their terminals and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PINs/PUKs, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

148 This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.CGA_SVD, OE.HID_VAD, OE.SCA_DTBS, OE.SVD_ Auth, OE.DTBS_Intend from Table 7 below for the eSign application.

[46] The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within the [IDCARDPP]

[47] 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].

[48] This rule is relevant for T.Skimming.

IV. ID_Card Holder Obligations

OE.ID_Card-Holder ID_Card Holder Obligations

149 The ID_Card Holder has to keep his or her verification values of eID-PIN and eID-PUK secret. The ID_Card Holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.
This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.Signatory from table below for the *eSign* application.

150 The PP ([IDCARDPP]) also includes all security objectives for the TOE's environment of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

151 For the sake of completeness the security objectives for the TOE's environment are listed below. More details can be found in the SSCD PP [SSCDPP].

Objective identifier	Comments
OE.SVD_Auth	concerns the following application(s): – eSign
OE.CGA_QCert	enforces the property #3 (CSP duties) of P.Trustworthy_PKI concerns the following application(s): – eSign
OE.DTBS_Intend	concerns the following application(s): – eSign
OE.Signatory	concerns the following application(s): – eSign
OE.SSCD_Prov_Service	concerns the following application(s): – eSign This environmental objective shall be achieved in such a way that (i) the CSP checks by means of the CGA, whether the device presented by the applicant for the (qualified) certificate examples holds unique identification as SSCD and is able to prove this identity; (ii) CGA detects alteration of the SVD imported from the TOE and verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the (qualified) certificate.
OE.HID_VAD	concerns the following application(s): – eSign This environmental objective shall be achieved in such a way that HID provides the human interface for user authentication and HID ensures confidentiality of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.
OE.DTBS_Protect	concerns the following application(s): – eSign This environmental shall be achieved in such a way that SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS representation cannot be altered undetected in transit between the SCA and the TOE.

Table 7: TOE's environment objectives taken over from [SSCDPP]

4.3 Security Objective Rationale

152 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.Identification	OT.Personalization	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Personalization	OE.Passive_Auth_Sign	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Terminal	OE.ID_Card-Holder	OE.Legislative_Compliance	OE.CGA_QCert ([SSCDPP])
T.Skimming			x	x	x										x	x	x		
T.Eavesdropping					x														
T.ID_Card_Tracing						x											x		
T.Forgery		x	x	x				x		x			x			x			
T.Counterfeit							x							x		x			
T.Abuse-Func								x											
T.Information_Leakage									x										
T.Phys-Tamper										x									
T.Malfunction											x								
P.Pre-Operational	x	x										x						x	
P.Terminal																x			
P.ID_Card_PKI													x	x					
P.Terminal_PKI															x				
P.Trustworthy_PKI													x		x				x

Table 8:Security Objective Rationale

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

154 The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the Service Provider) using the TOE's contactless interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the Terminal- and the Chip Authentication. The objective OE.Terminal_Authentication sets a prerequisite up for an effective terminal authentication (its property 'CVCAs must issue their certificates exclusively to the rightful organizations (DV) and DV must issue their certificates exclusively to the rightful equipment (terminals)'). The objective OE.Terminal sets a prerequisite up that no assets will be transferred between the TOE and the Service Provider before the Chip Authentication has successfully been accomplished (in its property 'Their (Service Provider's – remark given by the author of the PP) terminals

must not send assets (e.g. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the chip authentication'). The objective OE.ID_Card-Holder ensures that a PACE session can only be established either by the ID_Card holder itself or by an authorized person or device, and, hence, cannot be captured by an attacker.

155 The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective OT.Data_Confidentiality through the Chip Authentication.

156 The threat **T.ID_Card_Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of CAN, MRZ, eID-PIN and eID-PUK). This threat is directly countered by security objectives OT.ID_Card_Tracing (no gathering TOE tracing data) and OE.ID_Card-Holder (the attacker does not a priori know the correct values of the shared passwords).

157 The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the Service Provider. The security objective OT.Personalization requires the TOE to limit the write access for the ID_Card to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A Service Provider operating his terminals according to OE.Terminal and performing the Passive Authentication using the Card Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

158 The threat **T.Counterfeit** addresses the attack of unauthorized copy or reproduction of the genuine ID_Card. This attack is countered by the chip authenticity proof as aimed by OT.Chip_Auth_Proof using a chip authentication key pair to be generated within the issuing PKI branch as aimed by OE.Chip_Auth_Key. According to OE.Terminal the Service Provider's terminals has to perform the Chip Authentication Protocol to verify the authenticity of the ID_Card.

159 The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Prot_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

160 The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives OT.Prot_Inf_Leak**,** OT.Prot_Phys-Tamper and OT.Prot_Malfunction, respectively.

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

162 OT.Identification is affine to the OSP's property 'traceability before the operational phase';

163 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';

164 OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

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

166 The OSP **P.ID_Card_PKI** is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive_Auth_Sign (for the Card Security Object) and OE.Chip_\Auth_Key (for managing the ID_Card's Chip Authentication Key Pairs).

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

168 The OSP **P.Trustworthy_PKI** is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch), by OE.Terminal_Authentication (for CVCA, receiving PKI branch) and by OE.CGA_QCert (see [SSCDPP]).

169 The rationale related to the security objectives taken over from [SSCDPP] are exactly the same as given for the respective items of the security policy definitions in sec. 4.3 of [SSCDPP].

170 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)

171 They are all relevant and do not contradict Security Objectives of the TOE. They can be mapped to corresponding objectives of the TOE.

172 The remaining objective O.RND is covered by Security Objectives OT.Data_Integrity, and OT.Data_Confidentiality. These Security 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. Therefore this objective is supported by Security Objectives of the TOE.

173 The detailed analysis of Security Objectives derived from the hardware platform ST [HWST] and the environment of the Hardware Platform is made separately in chapter 7.10 (Statement of Compatibility).

5 Extended Components Definition

174 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]. Note that due to CC compatibility FPT_EMSEC is renamed in this ST to FPT_EMS.

5.1 FAU_SAS Audit data storage

175 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

176 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 FIA_API Authentication Proof of Identity

177 The family "Authentication Proof of Identity (FIA_API)" is specified as follows.

Family behavior:

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

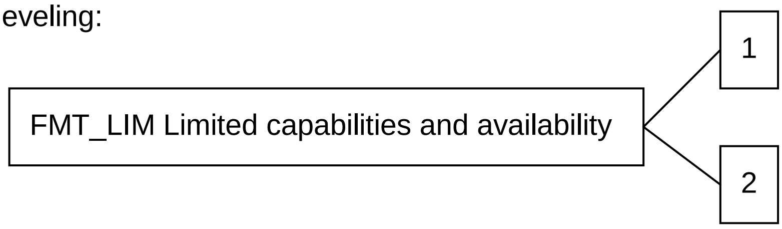
5.4 FMT_LIM Limited capabilities and availability

178 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.

5.5 FPT_EMS TOE Emanation

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

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMS.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_EMS.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

179 This part of the PP 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.

180 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.

181 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~~.

182 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *slanted and underlined*.

183 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *slanted and underlined*.

184 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.

185 In order to distinguish between the SFRs taken over from the SSCD PP [SSCDPP] and other SFRs having the same denotation, these SFRs are iterated by ‘/SSCD’ or ‘/XXX_SSCD’.

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

186 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	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT) – {FDP_ACC.1/Signature-creation_SFP_SSCD, FDP_ACF.1/Signature-

Security Functional Groups	Security Functional Requirements concerned
	creation_SFP_SSCD}
Secure data exchange between the ID_Card and the Service Provider connected	– FTP_ITC.1/CA: trusted channel Supported by: – FCS_COP.1/AES: encryption/decryption – FCS_COP.1/CMAC: MAC generation/verification – FIA_API.1/CA: Chip Identification/Authentication – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT) – FIA_UID.1/Rightful_Terminal: Terminal Identification (EIS, ATT, SGT) – FIA_UAU.1/PACE: PACE Authentication (PCT) – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT) – FIA_API.1/CA: Chip Identification/Authentication – FIA_UAU.4: single-use of authentication data – FIA_UAU.5: multiple authentication mechanisms – FIA_UAU.6: Re-authentication of Terminal – FIA_AFL.1/eID-PIN_Suspending – FIA_AFL.1/eID-PIN_Blocking: reaction to unsuccessful authentication attempts for establishing PACE communication using blocking authentication data – 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 ID_Card holder as Signatory (eSign-PIN) – FIA_UIA.1/SSCD: Authentication of ID_Card holder as Signatory (eSign-PIN) – FIA_AFL.1/SSCD: Blocking of the Signatory's RAD (eSign-PIN) Supported by: – FCS_CKM.1/DH_PACE: PACE authentication (PCT) – FCS_COP.1/SIG_VER: Terminal Authentication (EIS, ATT, SGT) – FCS_CKM.1/DH_CA: Chip Authentication – FCS_CKM.2/DH: Diffie-Hellmann key distribution within PACE and Chip authentication – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_COP.1/SHA: Keys derivation – FCS_RND.1: random numbers generation – FTP_ITC.1/PACE: preventing tracing while establishing Chip 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 the Signature Key Pair for the eSign application	– FCS_CKM.1/SSCD Supported by: – FCS_CKM.4/SSCD – {FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD, FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD} – {FDP_ACC.1/SVD_Transfer_SFP_SSCD, FDP_ACF.1/SVD_Transfer_SFP_SSCD}
Creation of Digital Signatures by the eSign application	– FCS_COP.1/SSCD
Management of and access to TSF and TSF-data	– The entire class FMT

Security Functional Groups	Security Functional Requirements concerned
	Supported by: – the entire class FIA: user identification/authentication – FCS_CKM.1.1/CA_PICC for CA key generation
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 9: Security functional groups vs. SFRs

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

Name	Data
Receiving PKI branch	
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [EACTR] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
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.
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the ID_Card issuer signs the Document Signer Public Key Certificate (C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA}) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK_{CSCA}). The CSCA also issues the self-signed Country Signing CertA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [ICAO9303-1], 5.1.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Card Security Object (SO_C) of the ID_Card with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS}).
Chip Authentication Public Key (PK_{PICC})	PK_{PICC} is stored in an EF on the ID_Card and used by the terminal for Chip Authentication. Its authenticity is verified by terminal in the context of the Passive Authentication (verification of SO_C).
Chip Authentication Private Key (SK_{PICC})	The Chip Authentication Key Pair (SK_{PICC}, PK_{PICC}) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman (ECDH, ECKA key agreement algorithm) according to [ECCTR, sec. A.2].

Name	Data
	SK_{PICC} is used by the TOE to authenticate itself as authentic ID_Card.
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, part 3 annexes A and E].
Chip Authentication Session Keys (CA-K_{MAC}, CA-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal (EIS, ATT, SGT) as result of the Chip Authentication Protocol, see [EACTR], sec. A.4, F.2.3.
Restricted Identification Keys	
Restricted Identification Key Pair {SK_{ID}, PK_{ID}}	Static Diffie-Hellman key pair, whereby the related private key SK_{ID} is stored in the TOE and used for generation of the sector-specific chip-identifier I_{ID}^{Sector} (pseudo-anonymization), see [EACTR, part 2 sec. 3.5]. This key represents user data within the current security policy. The belonging public key PK_{ID} is used for a revocation request and should not be stored in the TOE, see [EACTR, part 2 sec. 3.5].
Signature keys	
Signature Creation Key Pair (SCD/SVD)	Signature Creation Data (SCD) is represented by a private cryptographic key being used by the ID_Card 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 10: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

188 The following iterations are caused by different cryptographic key generation algorithms to be implemented and keys to be generated by the TOE.

189 **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][49] and specified cryptographic key sizes *128, 192 and 256*[50] that meet the following: [EACTR], part 3 Appendix A.3[51].

[49] [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]

[50] [assignment: *cryptographic key sizes*]

This item concerns the following application(s): ePassport, eID, eSign.

190 *Application Note 17:* The TOE generates a shared secret value with the terminal during the PACE Protocol, cf. [EACTR, part 1 sec. 3.2 and part 3 annex A.3]. The shared secret value is used to derive the AES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [EACTR, part 3 Appendix E] for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC. Note that a specified key size defines also the hash function used for key derivation.

191 *Application Note 18:* The TOE supports the following standardized elliptic curve domain parameters (cf. [EACTR, part 3 Table 4]):

ID	Name	Size	Reference
9	brainpoolP192r1	192	[RFC5639, 3.2]
11	brainpoolP224r1	224	[RFC5639, 3.3]
12	NIST P-256 (secp256r1)	256	[FIPS186, D.1.2.3]
13	brainpoolP256r1	256	[RFC5639, 3.4]
14	brainpoolP320r1	320	[RFC5639, 3.5]
16	brainpoolP384r1	384	[RFC5639, 3.6]
17	brainpoolP512r1	512	[RFC5639, 3.7]

192 FCS_CKM.1/DH_CA Cryptographic key generation – Diffie-Hellman Keys for Chip Authentication

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_CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to* [ECCTR][52] and specified cryptographic key sizes *128, 192 and 256*[53] that meet the following: [EACTR, part 3 Annex A.4][54].

This item concerns the following application(s): ePassport, eID, eSign.

193 *Application Note 19:* The TOE generates a shared secret value with the terminal during the CA Protocol, see [EACTR, part 1 sec. 3.4 and part 3 annex A.4], which uses standardized domain parameters listed in Application Note 18 on p. 48 (cf. [EACTR, part 3 Table 4]). The shared secret value is used to derive the AES session keys for message

[51] [assignment: *list of standards*]

[52] [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]

[53] [assignment: *cryptographic key sizes*]

[54] [assignment: *list of standards*]

encryption and message authentication (CA-K_{MAC}, CA-K_{Enc}) according to the [EACTR, part 3 annex E.2 and A.2] for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC. Note that a specified key size defines also the hash function used for key derivation.

194 FCS_CKM.1/CA_PICC Cryptographic key generation – Chip Authentication Key Pair

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA_PICC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA key generation compliant to* [ECCTR][55] and specified cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order*[56] that meet the following: [EACTR][57].

This item concerns the following application(s): ePassport, eID, eSign.

195 *Application Note 20:* The Chip Authentication Key Pair Generation operation is only available during Personalization Phase (Phase 3) (cf. FMT_MTD.1/SK_PICC) and not in Phase 4 “Operational Use”.

196 *Application Note 21:* This SFR for Chip Authentication Key Pair Generation operation is added according to the recommendation of the Protection Profile [IDCARDPP, *Application note 71*].

197 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.1/DH_CA
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

[55] [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]

[56] [assignment: *cryptographic key sizes*]

[57] [assignment: *list of standards*]

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[58] that meets the following:

1. PACE: as specified in [EACTR, part 2 sec. 3.2];
2. CA: as specified in [EACTR, part 2 sec. 3.3 and A.4][59].

This item concerns the following application(s): ePassport, eID, eSign.

198 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.1/DH_CA

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*[60] that meets the following: *none*[61].

This item concerns the following application(s): ePassport, eID, eSign.

199 *Application Note 22:* This SFR applies to the Session Keys, i.e. the TOE shall destroy the PACE Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the CA 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 also to the Chip Authentication Key SK_{PICC}, if generated by the Personalization Agent and the Signature Key SCD. The TOE will overwrite the assigned to the key memory data with the new key.

6.1.2.2 Cryptographic operation (FCS_COP.1)

200 The following iterations are caused by different cryptographic algorithms to be implemented by the TOE.

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

[58] [assignment: *cryptographic key distribution method*]

[59] [assignment: *list of standards*]

[60] [assignment: *cryptographic key destruction method*]

[61] [assignment: *list of standards*]

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[62] in accordance with a specified cryptographic algorithm *SHA-1 and SHA-256* [63] and cryptographic key sizes none[64] that meet the following: FIPS 180-2 [65].

This item concerns the following application(s): ePassport, eID, eSign.

202 *Application Note 23:* For hashing an ephemeral public key for DH (PACE[66] and CA[67]), the hash function SHA-1 will be used ([EACTR,part 3 Table 3]), but this is not relevant for the TOE. The TOE implements hash functions either SHA-1; SHA-224; SHA-256, SHA-384 or SHA-512 for the Terminal Authentication Protocol (cf. [EACTR, part 3 Table 14]). Within the normative Appendix E of [EACTR, part 3] '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.

203 FCS_COP.1/SIG_VER Cryptographic operation – Signature verification

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:

The root key PK_{CVCA} used for verifying C_{DV} is stored in the TOE during its personalisation (in the card issuing life phase). Since importing the respective certificates (C_T, C_{DV}) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the PP ([IDCARDPP]) does not contain any dedicated requirement like FDP_ITC.2 for the import function.

[62] [assignment: *list of cryptographic operations*]

[63] [assignment: *cryptographic algorithm*]

[64] [assignment: *cryptographic key sizes*]

[65] [assignment: *list of standards*]

[66] ID_{PICC} = H(ephem-PK_{PICC}-PACE) in [EACTR], sec. 4.4

[67] H(ephem-PK_{PCD}-TA) in [EACTR], sec. 4.3.1.2

FCS_CKM.4 Cryptographic key destruction: not fulfilled, but justified:

Cryptographic keys used for the purpose of the current SFR (PK_{PCD},PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret and, hence, needn't to be destroyed.

FCS_COP.1.1/ SIG_VER The TSF shall perform digital signature verification[68] in accordance with a specified cryptographic algorithm *ECDSA with plain signature format* [69] and cryptographic key sizes *192, 224, 256,320, 384 and 512 bit length group order* [70] that meet the following: [EACTR][71].

This item concerns the following application(s): ePassport, eID, eSign.

204 *Application Note 24:* The ECDSA with plain signature format is selected for the signature algorithm implemented by the TOE for the Terminal Authentication Protocol (cf. [EACTR, part 3 Appendix A.6] for details). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal generated a digital signature for the TOE challenge, see [EACTR, part 2 sec. 3.4]. The respective static public keys are imported within the respective certificates (C_T, C_{DV}) during the TA and are extracted by the TOE using PK_{CVCA} as the root key stored in the TOE during its personalization (see P.Terminal_PKI).

205 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.1/DH_CA
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[72] in accordance with a specified cryptographic algorithm AES in CBC mode[73] and cryptographic key sizes *128, 192 and 256 bit*[74] that meet the following: FIPS 197 [FIPS197] and [EACTR, part 3 Appendix E][75].

This item concerns the following application(s): ePassport, eID, eSign.

[68] [assignment: *list of cryptographic operations*]

[69] [assignment: *cryptographic algorithm*]

[70] [assignment: *cryptographic key sizes*]

[71] [assignment: *list of standards*]

[72] [assignment: *list of cryptographic operations*]

[73] [assignment: *cryptographic algorithm*]

[74] [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256]

[75] [assignment: *list of standards*]

206 *Application Note 25:* 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}) or the Chip Authentication Protocol according to the FCS_CKM.1/DH_CA (CA-K_{Enc}). Note that in accordance with [EACTR, part 3 Appendix E] 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 recommendend anymore by the BSI, Triple-DES is not applicable within the PP (cf. [IDCARDPP]).

207 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.1/DH_CA
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[76] in accordance with a specified cryptographic algorithm CMAC[77] and cryptographic key sizes *128, 192 or 256 bit*[78] that meet the following: [SP800-38B] and [EACTR, part 3 Appendix E[79].

This item concerns the following application(s): ePassport, eID, eSign.

208 *Application Note 26*: 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}) or the Chip Authentication Protocol according to the FCS_CKM.1/DH_CA (CA-K_{MAC}). Note that in accordance with [EACTR, Appendix E] DES could be used in Retail mode for secure messaging. Due to the fact that Retail-MAC is not recommendend anymore by the BSI, this algorithm is not applicable within the PP (cf. [IDCARDPP]).

6.1.2.3 Random Number Generation (FCS_RND.1)

209 FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

[76] [assignment: *list of cryptographic operations*]

[77] [assignment: *cryptographic algorithm*]

[78] [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit

[79] [assignment: *list of standards*]

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *the quality requirements for a DRG.4 generator according to* [AIS31][80].

This item concerns the following application(s): ePassport, eID, eSign.

210 Application Note 27: This requirement is specified in [AIS31] in more details. The TOE implements a hybrid deterministic random number generator of the pre-defined class DRG.4 that provides the following security capabilities (DRG.4.1 to DRG.4.5) with a defined quality metric (DRG.4.6 and DRG.4.7):

(DRG.4.1) The internal state of the RNG shall *use PTRNG of class PTG.2 as random source*[81].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy *on condition “session closed or aborted”*[82].

(DRG.4.5) The internal state of the RNG is seeded by *a PTRNG of class PTG.2*[83].

(DRG.4.6) The RNG generates output for which *$k > 2^{34}$*[84] strings of bit length 128 are mutually different with probability $1–\varepsilon$, with $\varepsilon < 2^{-16}$[85].

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A, *the NIST and the dieharder*[86] *tests*[87].

211 *Application Note 28*: This SFR requires the TOE to generate random numbers (random nonces) used for the authentication protocols PACE and TA as required by FIA_UAU.4.

212 *Application Note 29*: Chip Authentication, the (static and ephemeral) key generation and the challenge nonce generation during Personalization use directly the output of the PTG.2 provided by the hardware. For the security capabilities of this random number generator please refer to the hardware ST ([HWST]).

213 The PP ([IDCARDPP]) also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. For the functional class FCS there are the following components:

[80] [assignment: *a defined quality metric*]

[81] [selection: *use PTRNG of class PTG.2 as random source*, *have* [assignment: *work factor*], *require* [assignment: *guess work*]

[82] [selection: *on demand, on condition* [assignment: *condition*], *after* [assignment: *time*]]

[83] [selection: *internal entropy source, PTRNG of class PTG.2, PTRNG of class PTG.3,* [other selection]]

[84] [assignment: *number of strings*]

[85] [assignment: *probability*]

[86] The selected test suites http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.1.zip and http://www.phy.duke.edu/~rgb/General/dieharder/dieharder-3.31.0.tgz are available at NIST and Dieharder web sites. Note that the dieharder tests include Marsaglia’s “Diehard battery of tests” and NIST tests.

[87] [assignment: *additional test suites*]

SFR identifier	Comments
FCS_CKM.1/SSCD	concerns the following application(s): – eSign
FCS_CKM.4/SSCD	This SFR is covered by FCS_CKM.4. concerns the following application(s): – eSign
FCS_COP.1/SSCD	concerns the following application(s): – eSign

214 FCS_CKM.1/SSCD Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1/ SSCD The TSF shall generate **an SCD/SVD pair** ~~cryptographic keys~~ in accordance with a specified cryptographic key generation algorithm *ECDSA key generation compliant to* [ECCTR][88] and specified cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order* [89] that meet the following: [EACTR][90].

215 *Application Note 30:* The SCD/SVD Key Pair Generation requires authentication as Certification Service Provider (CSP) and is not available to other subjects (cf. FDP_\ ACC.1/SCD/SVD_Generation_SFP_SSCD. The refinement substitutes “cryptographic keys” by “SCD/SVD pairs” because it clearly addresses the SCD/SVD key generation.

216 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 FCS_CKM.1/SSCD
FCS_CKM.4 Cryptographic key destruction]: fulfilled by FCS_CKM.4/SSCD.

[88] [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]

[89] [assignment: *cryptographic key sizes*]

[90] [assignment: *list of standards*]

FCS_COP.1.1/ SSCD The TSF shall perform digital signature generation[91] in accordance with a specified cryptographic algorithm *ECDSA compliant to* [ECCTR][92] and cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order*[93] that meet the following: [ECCTR][94].

6.1.3 Class FIA Identification and Authentication

217 *Application Note 31:* The Table 11 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/eID-PIN_Suspending FIA_AFL.1/eID-PIN_Blocking FIA_AFL.1/PACE	as required by FCS_CKM.1/DH_PACE
Terminal Authentication Protocol	FIA_UAU.1/Rightful_Terminal FIA_UAU.5	as required by FCS_COP.1/SIG_VER
Chip Authentication Protocol	FIA_API.1/CA, FIA_UAU.5, FIA_UAU.6	as required by FCS_CKM.1/DH_CA
eSign-PIN	FIA_UAU.1/SSCD	-

Table 11: Overview of authentication SFRs

218 FIA_AFL.1/eID-PIN_Suspending Authentication failure handling – Suspending eID-PIN

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 *an administrator configurable positive integer s_{ad} within the range* $1 \le s_{ad} \le 6$ *according to* [TCOSADM] [95] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using eID-PIN as the shared password for PACE[96].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[97], the TSF shall suspend the reference value of eID-PIN according to [EACTR, part 2 sec. 2.3.1][98].

[91] [assignment: *list of cryptographic operations*]

[92] [assignment: *cryptographic algorithm*]

[93] [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit

[94] [assignment: *list of standards*]

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

[96] [assignment: *list of authentication events*]

[97] [selection: *met, surpassed*]

This item concerns the following application(s): eID, eSign.

219 According to [EACTR, part 2 sec. 2.3.1], at least the current value 1 of the retry counter for eID-PIN shall be a *suspending* value, i.e. if this value is reached the eID-PIN *must* be suspended. Nevertheless the administrator may select a different suspending value and a corresponding initial value. The assignment must be according with requirements given in [TCOSADM].

220 FIA_AFL.1/eID-PIN_Blocking Authentication failure handling – Blocking eID-PIN

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 *an administrator configurable positive integer b_{ad} within the range* $1 \le b_{ad} \le 3$ *according* [TCOSADM][99] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using suspended eID-PIN as the shared password for PACE[100].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[101], the TSF shall block the reference value of eID-PIN according to [EACTR, part 2 sec. 2.3.1][102].

This item concerns the following application(s): eID.

221 *Application Note 32:* According to [EACTR, part 2 sec. 2.3.1], the eID-PIN must be in the *suspending* state if the current value of the retry counter RC is 1, the *blocking* current value of the retry counter for eID-PIN shall be RC = 0. Nevertheless the administrator may configure the TOE such that it suspends already the eID-PIN if the retry counter reaches the value b_{ad}. The assignment shall be consistent with the implemented authentication mechanism and resistant against attacks with high attack potential. No more then $b_{ad} + s_{ad} \le 9$ overall tries of the eID-PIN are allowed.

222 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

[98] [assignment: *list of actions*]

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

[100] [assignment: *list of authentication events*]

[101] [selection: *met, surpassed*]

[102] [assignment: *list of actions*]

FIA_AFL.1.1 The TSF shall detect when *1*[103] unsuccessful authentication attempts occur related to authentication attempts using CAN, MRZ, eID-PUK as shared passwords for PACE[104].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[105], the TSF shall *require the restart of the PACE protocol, and the TSF increases depending on the PACE password used the reaction time to the next authentication attempt*[106]*.*

This item concerns the following application(s): ePassport, eID, eSign.

223 *Application Note 33*: The assignment operation reflects the fact that according the implementation the authentication procedure consumes a defined minimal amount of time. Because MRZ and eID-PUK 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 9 digit number would require already about 30 years). Since the CAN with lower entropy does not represent a secret, because it may be revealed already to external entities (cf. footnote 13 on p. 18) it might be not necessary to consider a brute force attack against the CAN. The waiting time after power-up is sufficient to prevent the skimming of the TOE even for a random 6 digit CAN value if the Attacker does not know the CAN.

224 *Application Note 34*: The TOE detects any unsuccessful authentication attempt. After a administrator configurable number of authentication failures with the CAN has been met, the TSF adds an extra time before it allows for the next PACE run with the CAN (cf. [TCOSADM]).

225 FIA_API.1/CA Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide the Chip Authentication Protocol according to [EACTR, part 2 sec. 3.3] [107] to prove the identity of the TOE[108].

This item concerns the following application(s): ePassport, eID, eSign.

226 *Application Note 35:* The Chip Authentication shall be triggered by the rightful terminal immediately after the successful Terminal Authentication (as required FIA_UAU.1/ Rightful_Terminal) using, amongst other, H(ephem-PK_{PCD}-TA) from the accomplished TA. The terminal verifies genuineness of the ID_Card by verifying the authentication token T_{PICC} calculated by the ID_Card using ephem-PK_{PCD}-TA and CA-K_{MAC}, (and, hence, finally

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

[104] [assignment: *list of authentication events*]

[105] [selection: *met, surpassed*]

[106] [assignment: *list of actions*]

[107] [assignment: *authentication mechanism*]

[108] [assignment: *authorized user or role*]

making evident possessing the Chip Authentication Key (SK_{PICC})).
The Passive Authentication making evident authenticity of the PK_{PICC} by verifying the Card Security Object (SO_C) up to CSCA shall be triggered by the rightful terminal immediately after the successful Terminal Authentication before the Chip Authentication[109] and is considered to be part of the CA Protocol (see also P.Terminal).
Please note that this SFR does not require authentication of any TOE's user, but providing evidence enabling an external entity (the terminal connected) to prove the TOE's identity.
If the Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc}), cf. FTP_ITC.1/CA. Otherwise, Secure Messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

227 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, part 1 sec. 3.3[110]

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.

This item concerns the following application(s): ePassport, eID, eSign.

228 *Application Note 36:* The user identified after a successfully performed PACE protocol is a PACE terminal (PCT). In case eID-PIN or eID-PUK were used for PACE, it is the ID_Card holder using PCT. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. in case CAN or MRZ were used for PACE, it is either the ID_Card holder itself or an authorized other person or device.

229 FIA_UID.1/Rightful_Terminal 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, part 1

[109] cf. [EACTR], sec. 3.4

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

	<u>sec. 3.3],</u> 3. <u>carrying out the Terminal Authentication Protocol according to [EACTR, part 2 sec. 3.4]</u>[111] 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.

This item concerns the following application(s): ePassport, eID, eSign.

230 *Application Note 37:* The user identified after a successfully performed TA protocol is a rightful terminal, i.e. either EIS or ATT or SGT.

231 *Application Note 38:* 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.
Please note that a Personalization Agent acts on behalf of the ID_Card Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalization Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role ‘Personalization Agent’, when a terminal (e.g. ATT) proves the respective Terminal Authorization Level.

232 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. <u>establishing a communication channel,</u> 2. <u>carrying out the PACE Protocol</u>[112] <u>according to [EACTR, part 1 sec. 3.3]</u>[113] 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.

This item concerns the following application(s): ePassport, eID, eSign.

233 *Application Note 39:* The user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). In case eID-PIN or eID-PUK were used for PACE, it is the ID_Card holder using PCT. Please note that neither CAN nor MRZ effectively represent

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

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

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

secrets, but are restricted-revealable; i.e. in case CAN or MRZ were used for PACE, it is either the ID_Card holder itself or an authorized other person or device.
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.

234 FIA_UAU.1/Rightful_Terminal Timing of authentication

Hierarchical to: No other components.

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

FIA_UAU.1.1/ Rightful_Terminal The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE protocol according to [EACTR, part 1 sec. 3.3,
3. carrying out the Terminal Authentication Protocol[114] according to [EACTR, part 2 sec. 3.4] [115]

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

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

This item concerns the following application(s): ePassport, eID, eSign.

235 *Application Note 40:* The user authenticated after a successfully performed TA protocol is a Service Provider represented by a rightful terminal, i.e. either EIS or ATT or SGT. The authenticated terminal will immediately perform the Chip Authentication (Version 2) as required by FIA_API.1/CA using, amongst other, H(ephem-PK_{PCD}-TA) from the accomplished TA. Please note that the Passive Authentication is considered to be part of the CA protocol within the PP [IDCARDPP].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to[EACTR, part 1 sec. 3.3],
2. Terminal Authentication Protocol according to [EACTR, part 2 sec. 3.4][116].

[114] ID_Card identifies themselves within the TA protocol by using the identifier ID_{PICC} = H(ephem-PK_{PICC}-PACE).

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

This item concerns the following application(s): ePassport, eID, eSign.

237 *Application Note 41:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length length being (almost) uniformly distributed (the PP [IDCARDPP] supports the key derivation function based on AES; see [EACTR, part 3 annexes A.2 and E]). For the TA protocol, TOE randomly selects a nonce r_{PICC} of 64 bits length, see [EACTR, part 3 annex B].

238 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, part 1 sec. 3.3],
2. Terminal Authentication Protocol according to [EACTR, part 2 sec. 3.4],
3. Chip Authentication Protocol according to [EACTR, part 2 sec. 3.3],

and

4. Secure messaging in encrypt-then-authenticate mode according to [EACTR, part 3 Appendix E[117]

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 by means of the Terminal Authentication Protocol, only if (i) the terminal presents its static public key[118] being successfully verifiable up to CVCA and (ii) the terminal uses the PICC identifier[119] calculated during and the secure messaging established by the current PACE authentication.
2. Having successfully run the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the Chip Authentication Protocol[120].

This item concerns the following application(s): ePassport, eID, eSign.

[116] [assignment: *identified authentication mechanism(s)*]

[117] [assignment: *list of multiple authentication mechanisms*]

[118] PK_{PCD}

[119] ID_{PICC} = H(ephem-PK_{PICC}-PACE)

[120] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

239 *Application Note 42:* Please note that Chip Authentication Protocol does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the TOE's identity.

240 *Application Note 43:* 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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 Chip Authentication Protocol shall be verified as being sent by the rightful terminal[121].

This item concerns the following application(s): ePassport, eID, eSign.

242 *Application Note 44:* The PACE and the Chip Authentication Protocols as specified in [EACTR] start secure messaging used for all commands exchanged after successful PACE authentication and CA. 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. For the Terminal Authentication, the current secure messaging session is bounded on H(ephem-PK_{PCD}-TA).

243 The PP ([IDCARDPP]) also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. For the functional class FIA there are the following components:

244 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, cf. [SSCDPP]

FIA_UAU.1.1/ The TSF shall allow

[121] [assignment: *list of conditions under which re-authentication is required*]

SSCD

1. self test according to FPT_TST.1,
2. identification of the user by means of TSF required by FIA_UID.1/SSCD in [SSCDPP]
3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA[122],
4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA[123],
5. *none*[124]

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.

This item concerns the following application(s): ePassport, eID, eSign.

SFR identifier	Comments
FIA_UID.1/SSCD	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any. concerns the following application(s): – eSign
FIA_AFL.1/SSCD	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any. concerns the following application(s): – eSign

245 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* [125]

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.

[122] the authenticated terminal is ATT, cf. FIA_UAU.1/Rightful_Terminal

[123] the authenticated terminal is SGT, cf. FIA_UAU.1/Rightful_Terminal; the trusted channel by FTP_ITC.1/CA implements a trusted path between HID and the TOE.

[124] [assignment: *list of (additional) TSF-mediated actions*]

[125] [assignment: *list of additional TSF-mediated actions*]

246 FIA_AFL.1/SSCD Authentication failure handling

Hierarchical to: No other components.

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

FIA_AFL.1.1/SSCD The TSF shall detect when *an administrator configurable positive integer* sig_{ad} *within the range* $1 \leq sig_{ad} \leq 9$ *according to* [TCOSADM][126] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[127].

FIA_AFL.1.2/SSCD When the defined number of unsuccessful authentication attempts has been met[128], the TSF shall block RAD[129].

6.1.4 Class FDP User Data Protection

247 FDP_ACC.1/TRM Subset access control – Terminal Access

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDF_ACF.1/TRM

FDP_ACC.1.1/TRM The TSF shall enforce the Terminal Access Control SFP [130] on terminals gaining write, read, modification and usage access to the User Data stored in the ID_Card [131].

This item concerns the following application(s): ePassport, eID, eSign.

248 FDP_ACF.1/TRM Security attribute based access control – Terminal Access

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM
FMT_MSA.3 Static attribute initialization: not fulfilled, but **justified:**
The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personali-

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

[127] [assignment: *list of authentication events*]

[128] [selection: *met, surpassed*]

[129] [assignment: *list of actions*]

[130] [assignment: *access control SFP*]

[131] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

zation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

FDP_ACF.1.1/TRM The TSF shall enforce the Terminal Access Control SFP[132] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. PACE Terminal (PCT),
   c. Rightful Terminal (EIS, ATT, SGT);
2. Objects:

   User Data stored in the TOE;
3. Security attributes:
   a. Authentication status of terminals,
   b. Terminal Authorization Level,
   c. CA authentication status,
   d. Authentication status of the ID_Card holder as Signatory (if the *eSign* is operational) [133].

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. a successfully authenticated Extended Inspection System (EIS) is allowed to read User Data according to [EACTR, part 3 sec. C.4] after a successful CA as required by FIA_API.1/CA,
2. a successfully authenticated Authentication Terminal (ATT) is allowed to read, modify and write User Data as well as to generate signature key pair(s) within the eSign application (SCD/SVD Generation[134]) according to [EACTR, part 3 sec. C.4] after a successful CA as required by FIA_API.1/CA,
3 a successfully authenticated Signature Terminal (SGT) is allowed to use the private signature key within the eSign application (SCD) for generating digital signatures according to [EACTR, part 3 sec. C.4] after a successful CA as required by FIA_API.1/CA and a successful authentication of the ID_Card holder as Signatory as required by FIA_UAU.1/SSCD[135].

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[136].

[132] [assignment: *access control SFP*]

[133] [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*]

[134] as required by FCS_CKM.1/SSCD

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

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

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. Any terminal (including PCT) being not authenticated as a rightful terminal (i.e. as either EIS or ATT or SGT) is not allowed to read, to write, to modify, to use any User Data stored on the ID_Card.
2. Nobody is allowed to read ‘TOE immanent secret cryptographic keys’ stored on the ID_Card.
3. Nobody is allowed to read ‘secret ID_Card holder authentication data’ stored on the ID_Card.
4. Nobody is allowed to read the private Restricted Identification (SK_{ID}) key stored on the ID_Card.
5. Nobody is allowed to read the private signature key(s) within the eSign application (SCD; if the *eSign* application is operational[137].

This item concerns the following application(s): ePassport, eID, eSign.

249 *Application Note 45*: The relative certificate holder (Service Provider) authorization is encoded in the Card Verifiable Certificate of the terminals being operated by the Service Provider. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Terminal Certificate (cf. FMT_MTD.3). The Terminal Authorization Level is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Terminal Certificate in a valid certificate chain. It is technically based on Certificate Holder Authorization Template (CHAT), see [EACTR, part 3 sec C.1]. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ID_Card holder’s restricting input at the terminal. This final CHAT reflects the *effective authorization level*, see [EACTR, part 3 sec. C.4.2] and is then sent to the TOE by the command 'MSE:Set AT' within the Terminal Authentication (B.3 und B.11.1 of [EACTR, part 3]).

250 *Application note 46*: Please note that the General Authentication Procedure as required by FIA_UAU.5 is mandatory for all the applications residing on the TOE, see [EACTR, part 2 sec. 2.4]. Note that the IDCARDPP supports only [EACTR, part 2], whereby EAC shall be mandatory for all user data (DG1 – DG16) of the *ePassport*.
Please note that the Card Security Object (SO_C) does not belong to the user data, but to the TSF data. The Card Security Object can be read out by the PCT, see [EACTR, part 3 sec. A.1.2] for EF.CardSecurity.

251 *Application Note 47*: Please note that this functional requirement also covers the ability to activate the *eSign* application using the ATT with an appropriate Terminal Authorization Level, see [EACTR, part 3 sec. C.4] and acting on behalf of the CSP and upon an application by the ID_Card holder.

252 *Application note 48*: Please note that the control on the user data transmitted between the TOE and the rightful terminal is addressed by FTP_ITC.1/CA.

253 FDP_RIP.1 Subset residual information protection

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

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[138] the following objects:

1. the Chip Authentication Private Key (SK$_{PICC}$),
2. the secret ID_Card holder authentication data eID-PIN, eID-PUK, eSign-PIN (RAD, if *eSign* application is operational),
3. the session keys (PACE-K$_{MAC}$, PACE-K$_{Enc}$), (CA-K$_{MAC}$, CA-K$_{Enc}$)
4. the private Restricted Identification key SK$_{ID}$,
5. the private signature key of the ID_Card holder (SCD; if the *eSign* application is operational)
6. *none*[139].

This item concerns the following application(s): ePassport, eID, eSign.

254 *Application Note 49*: 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_EMS.

255 *Application Note 50*: Please note that FDP_RIP.1 also contributes to achievement of OT.Sigy_SigF (eSign-PIN) and OT.SCD_Secrecy (SCD) from [SSCDPP].

256 The PP ([IDCARDPP]) also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. For the functional class FDP there are the following components:

SFR identifier	Comments
FDP_ACC.1/SCD/SVD_Generation_SFP_ SSCD	concerns the following application(s): – eSign
FDP_ACF.1/SCD/SVD_Generation_SFP_ SSCD	concerns the following application(s): – eSign
FDP_ACC.1/SVD_Transfer_SFP_SSCD	concerns the following application(s): – eSign
FDP_ACF.1/SVD_Transfer_SFP_SSCD	concerns the following application(s): – eSign
FDP_ACC.1/Signature-creation_SFP_SSCD	concerns the following application(s): – eSign
FDP_ACF.1/Signature-creation_SFP_SSCD	concerns the following application(s): – eSign
FDP_RIP.1/SSCD	This item is covered by FDP_RIP.1 concerns the following application(s): – eSign
FDP_SDI.2/Persistent_SSCD	concerns the following application(s): – eSign
FDP_SDI.2/DTBS_SSCD	concerns the following application(s):

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

[139] [assignment: *list of objects*]

SFR identifier	Comments
	– eSign

257 The following security attributes and related status for the subjects and objects defined in the SSCD PP [SSCDPP] are applicable, if the *eSign* application is operational:

Subject / Object	Security attribute type	Values of the attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD / SVD Management	authorized, not authorized
SCD	SCD Operational	no, yes
SCD	SCD Identifier	arbitrary value

258 *Application Note 51*: 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.

259 FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD Subset access control

Hierarchical to: No other components.

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

FDP_ACC.1.1/SCD/SVD_Generation_SFP_SSCD The TSF shall enforce the SCD/SVD Generation SFP[140] on

1. subjects: S.User
2. objects: SCD, SVD
3. operations: generation of SCD/SVD pair[141].

260 FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD Security attribute based access control

Hierarchical to: No other components.

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

[140] [assignment: *access control SFP*]

[141] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FDP_ACF.1.1/SCD/SVD_Generation_SFP_ SSCD The TSF shall enforce the SCD/SVD_Generation_SFP[142] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[143].

FDP_ACF.1.2/SCD/SVD_Generation_SFP_ SSCD The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

> S.User with the security attribute "SCD/SVD Management" set to "authorized" is allowed to generate SCD/SVD pair[144].

FDP_ACF.1.3/SCD/SVD_Generation_SFP_ SSCD The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[145].

FDP_ACF.1.4/SCD/SVD_Generation_SFP_ SSCD The TSF shall explicitly deny access of subjects to objects The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

> S.User with the security attribute "SCD/SVD management" set to "not authorized" is not allowed to generate SCD/SVD pair[146].

261 FDP_ACC.1/SVD_Transfer_SFP_SSCD Subset access control

Hierarchical to: No other components.

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

FDP_ACC.1.1/SVD_Transfer_SFP_SSCD The TSF shall enforce the SVD_Transfer_SFP[147] on

1. subjects: S.User,
2. objects: SVD,
3. operations: export[148].

262 FDP_ACF.1/SVD_Transfer_SFP_SSCD Security attribute based access control

Hierarchical to: No other components.

[142] [assignment: *access control SFP*]

[143] [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*]

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

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

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

[147] [assignment: *access control SFP*]

[148] [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_ACF.1/SVD_Transfer_SFP_SSCD,
FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCD

FDP_ACF.1.1/ SVD_Transfer_SFP The TSF shall enforce the SVD_Transfer_SFP[149] to objects based on the following:

1. the S.User is associated with the security attribute Role,
2. the SVD[150].

FDP_ACF.1.2/ SVD_Transfer_ SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin* [151] is allowed to export SVD[152].

FDP_ACF.1.3/ SVD_Transfer_ SFP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[153].

FDP_ACF.1.4/ SVD_Transfer_ SFP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[154].

263 FDP_ACC.1/Signature_Creation_SFP_SSCD 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_SSCD

FDP_ACC.1.1/_Signature-creation_ SFP_SSCD The TSF shall enforce the Signature-creation_SFP[155] on

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature-creation[156].

264 FDP_ACF.1/ Signature_Creation_SFP_SSCD Security attribute based access control

Hierarchical to: No other components.

[149] [assignment: *access control SFP*]

[150] [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*]

[151] [selection: *R.Admin, R.Sigy*]

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

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

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

[155] [assignment: *access control SFP*]

[156] [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_SSCD, FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCD

FDP_ACF.1.1/_Signature-creation_SFP_SSCD	The TSF shall enforce the Signature-creation_SFP[157] 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"[158].
FDP_ACF.1.2/ Signature-creation_SFP_SSCD	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 [159].
FDP_ACF.1.3/ Signature-creation_SFP_SSCD	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[160].
FDP_ACF.1.4/ Signature-creation_SFP_SSCD	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"[161].

265 FDP_SDI.2/Persistent_SSCD Stored data integrity monitoring and action

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[162] on all objects, based on the following attributes: integrity checked stored data[163].
FDP_SDI.2.2/ Persistent_SSCD	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data

[157] [assignment: *access control SFP*]

[158] [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*]

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

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

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

[162] [assignment: *integrity errors*]

[163] [assignment: *user data attributes*]

2. inform the S.Sigy about integrity error[164].

266 FDP_SDI.2/DTBS_SSCD Stored data integrity monitoring and ction

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[165] on all objects, based on the following attributes: integrity checked stored DTBS[166].

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[167].

6.1.5 Class FTP Trusted Path/Channels

267 FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **PACE terminal (PCT) 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 The TSF shall permit ~~another trusted IT product~~ **the PCT** [168] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the PCT after PACE[169].

This item concerns the following application(s): ePassport, eID, eSign.

268 *Application note 52*: 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-

[164] [assignment: *action to be taken*]

[165] [assignment: *integrity errors*]

[166] [assignment: *user data attributes*]

[167] [assignment: *action to be taken*]

[168] [selection: *the TSF, another trusted IT product*]

[169] [assignment: *list of functions for which a trusted channel is required*]

K_{Enc}): this secure messaging enforces preventing tracing while establishing Chip Authentication; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/AES and FCS_COP.1/CMAC.
The PACE secure messaging session is immediately superseded by a CA secure messaging session after successful Chip Authentication as required by FTP_ITC.1/CA.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE and FIA_AFL.1/eID-PIN_Blocking.

269 FTP_ITC.1/CA Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **rightful terminal (EIS, ATT, SGT) after Chip Authentication** 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/CA The TSF shall permit ~~another trusted IT product~~ **the rightful terminal (EIS, ATT, SGT)**[170] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for <u>any data exchange between the TOE and the Service Provider represented by the rightful terminal after Chip Authentication</u>[171].

This item concerns the following application(s): ePassport, eID, eSign.

270 *Application note 53*: The trusted IT product is the Terminal. In FTP_ITC.1.3/PACE, the word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

271 *Application Note 54*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE), the TA protocol (FIA_UAU.1/Rightful_Terminal) and the CA protocol (FIA_API.1/CA). If the Chip Authentication was successfully performed, Secure Messaging is restarted immediately using the derived session keys {CA-K_{MAC}, CA-K_{Enc}}[172]: this secure messaging enforces the required properties of the operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/AES and FCS_COP.1/CMAC.

272 *Application Note 55*: Please note that the communication channel being established between the ID_Card and the PACE Terminal also uses secure messaging (with {PACE-

[170] [selection: *the TSF, another trusted IT product*]

[171] [assignment: *list of functions for which a trusted channel is required*]

[172] otherwise, Secure Messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE

K_{MAC}, PACE-K_{Enc}}) being itself enough strong for the current security policy. Nevertheless, the PP ([IDCARDPP]) does not cover the PACE trusted channel due to the circumstance that short, non-blocking authorization data CAN and MRZ can be used for starting (and also hijacking) a PACE-session, so that the establishing phase of the PACE trusted channel is not sufficiently strong for the current security policy (please refer to T.Skimming). The PACE secure messaging session is immediately superseded by the CA secure messaging session after successful Chip Authentication as required by FTP_ITC.1/CA.

273 *Application Note 56*: Please note that the control on user data stored in the TOE is addressed by FDP_ACF.1/TRM.

274 *Application note 57*: The requirement FTP_ITC.1/CA also covers a secure transport of (i) SVD[173] from the TOE to CGA[174] as well as of (ii) VAD[175] from HID[176] and of (iii) DTBS[177] from SCA to the TOE. It also covers TOE's capability to generate and to provide CGA with evidence that can be used as a guarantee of the validity of SVD. The current SFR reflects the main additional feature concerning the *eSign* application comparing to [SSCDPP].

6.1.6 Class FAU Security Audit

275 FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[178] with the capability to store the Initialization and Pre-Personalization Data[179] in the audit records.

This item concerns the following application(s): ePassport, eID, eSign.

276 *Application Note 58*: The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the ID_Card 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 ID_Card (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.

[173] integrity is to secure

[174] the authenticated terminal is ATT with bits 7 (install qualified certificate) or/and 6 (install certificate) set to 1, cf. [EACTR], sec. C.4.1.2.

[175] confidentiality is to secure

[176] the authenticated terminal is SGT

[177] integrity is to secure

[178] [assignment: *authorized users*]

[179] [assignment: *list of audit information*]

6.1.7 Class FMT Security Management

277 *Application Note 59*: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

278 **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,
4. Resume and unblock the eID-PIN[180],
5. Activate and deactivate the eID-PIN[181].

This item concerns the following application(s): ePassport, eID, eSign.

279 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

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

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. Terminal,
6. PACE Terminal (PCT),
7. (Extended) Inspection System (EIS),
8. Authentication Terminal (ATT),
9. Signature Terminal (SGT),
10. ID_Card holder[182].

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

[180] unblocking eSign-PIN is managed by FMT_SMF.1/SSCD

[181] [assignment: *list of management functions to be provided by the TSF*]

[182] [assignment: *the authorized identified roles*]

This item concerns the following application(s): ePassport, eID, eSign.

280 *Application Note 60*: For the explanation on the role Manufacturer please refer to the *Application Note 58*; on the role Personalization Agent – to the *Application Note 38*. The role Terminal is the default role for any terminal being recognized by the TOE as neither PCT nor EIS nor ATT nor SGT (‘Terminal’ is used by the ID_Card presenter). The). The roles CVCA, DV, EIS, ATT[183] and SGT are recognized by analyzing the current Terminal Certificate C_T, cf. [EACTR, part 3 C.4] (FIA_UID.1/ Rightful_Terminal). The TOE recognizes the ID_Card holder by using PCT upon input eID-PIN or eID-PUK (FIA_UID.1/ PACE) as well as – in the context of the eSign application – by using SGT upon input VAD (eSign-PIN) governed by FIA_UAU.1/SSCD .

281 *Application Note 61*: 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.

282 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[184].

This item concerns the following application(s): ePassport, eID, eSign.

283 FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

[183] ATT plays a special role ‘CGA’ for the *eSign* application, if bits 7 (install qualified certificate) or/and 6 (install certificate) are set to 1 within the effective terminal authorisation level, cf. .[EACTR], sec. C.4.1.2; an ATT with such an terminal authorisation level is authorized by the related CSP to act as CGA on its behalf.

[184] [assignment: *Limited capability and availability policy*]

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[185].

This item concerns the following application(s): ePassport, eID, eSign.

284 FMT_MTD.1/INI_ENA Management of TSF data – Writing 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_ENA The TSF shall restrict the ability to write[186] the Initialization Data and Pre-personalization Data[187] to the Manufacturer[188].

This item concerns the following application(s): ePassport, eID, eSign.

285 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[189] the Initialization Data[190] to the Personalization Agent[191].

This item concerns the following application(s): ePassport, eID, eSign.

[185] [assignment: *Limited capability and availability policy*]

[186] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[187] [assignment: *list of TSF data*]

[188] [assignment: *the authorized identified roles*]

[189] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[190] [assignment: *list of TSF data*]

[191] [assignment: *the authorized identified roles*]

286 *Application Note 62:* 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 phase 'operational use'. Please also refer to the *Application Note 38*.

287 FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

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/ CVCA_INI The TSF shall restrict the ability to write[192] the

1. initial Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the initial Country Verifying Certification Authority Certificate (C_{CVCA}), as required in [EACTR, part 3 sec. A.6]
3. initial Current Date
4. *none*[193]

to *the Personalization Agent*[194].

This item concerns the following application(s): ePassport, eID, eSign.

288 *Application Note 63:* The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent in the issuing phase (cf. [EACTR, sec. 2.2.4). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The metadata of the initial Country Verifying Certification Authority Certificate and the initial Current Date are needed for verification of the certificates and the calculation of the Terminal Authorization Level. Please note that only a *subset* of the metadata must be stored in the TOE, see [EACTR, sec. A.6.2.3]; storing of further certificate's content is optional. In fact it is not the initial CVCA Certificate, which is necessary for verification, but the public key included therein, and the self-signature gives no additional security. Therefore the TOE will expect the initial CVCA Certificate to be written by the Personalization Agent without the self-signature (cf. [TCOSADM]).

[192] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[193] [assignment: *list of TSF data*]

[194] [assignment: *the authorized identified roles*]

289 FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority

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/ CVCA_UPD The TSF shall restrict the ability to update[195] the

1. Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the Country Verifying Certification Authority Certificate (C_{CVCA}) as required in [EACTR, sec. A.6.2.3]
3. *none*[196]

to Country Verifying Certification Authority[197].

This item concerns the following application(s): ePassport, eID, eSign.

290 *Application Note 64:* The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key and the related metadata by means of the CVCA Link-Certificates (cf. [EACTR], sec. 2.2). The TOE updates its internal trust-point, if a valid CVCA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [EACTR], sec. 2.2.3 and 2.2.4).

291 FMT_MTD.1/DATE Management of TSF data – Current date

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/ DATE The TSF shall restrict the ability to modify[198] the Current Date[199] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Rightful Terminal (EIS, ATT or SGT) possessing an Accurate Terminal Certificate[200].

This item concerns the following application(s): ePassport, eID, eSign.

292 *Application Note 65*: The authorized roles are identified in their certificates (cf. [EACTR], sec. 2.2.4 and C.4) and authorized by validation of the certificate chain up to CVCA (cf.

[195] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[196] [assignment: *list of TSF data*]
[197] [assignment: *the authorized identified roles*]
[198] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[199] [assignment: *list of TSF data*]
[200] [assignment: *the authorized identified roles*]

FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. [EACTR], A.6 for details).

293 FMT_MTD.1/PA_UPD Management of TSF data – Personalization Agent

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/PA_UPD The TSF shall restrict the ability to write[201] the Card Security Object (SO_C)[202] to the Personalization Agent[203].

This item concerns the following application(s): ePassport, eID, eSign.

294 *Application Note* 66: Please refer to the *Application Note 38*.

295 FMT_MTD.1/SK_PICC Management of TSF data – Chip Authentication Private Key

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/SK_PICC The TSF shall restrict the ability to *load or create*[204] the Chip Authentication Private Key (SK_{PICC})[205] to *Personalization Agent*[206].

This item concerns the following application(s): ePassport, eID, eSign.

296 *Application Note 67:* The component FMT_MTD.1/SK_PICC is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load”. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. This is the default operation. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself during Personalization. This operation is no more available after Personalization.

[201] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[202] [assignment: *list of TSF data*]
[203] [assignment: *the authorized identified roles*]
[204] [selection: create, load]/[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[205] [assignment: *list of TSF data*]
[206] [assignment: *the authorized identified roles*]

297 FMT_MTD.1/KEY_READ Management of TSF data – Private Key Read

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1.

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read[207] the Chip Authentication Private Key (SK_{PICC})[208] to none[209].

This item concerns the following application(s): ePassport, eID, eSign.

298 FMT_MTD.1/eID-PIN_Resume Management of TSF data – Resuming eID-PIN

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1.

FMT_MTD.1.1/ eID-PIN_Resume The TSF shall restrict the ability to resume[210] the suspended eID-PIN[211] to the ID_Card holder[212].

This item concerns the following application(s): eID.

299 *Application Note 68:* The resuming procedure is a two-step one subsequently using PACE with CAN and PACE with eID-PIN. It must be implemented according to [EACTR], sec. 3.5.1 and is relevant for the status as required by FIA_AFL.1/eID-PIN_Suspending. The ID_Card holder is authenticated as required by FIA_UAU.1/PACE using the eID-PIN as the shared password.

300 FMT_MTD.1/eID-PIN_Unblock Management of TSF data – Unblocking eID-PIN

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1.

[207] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[208] [assignment: *list of TSF data*]
[209] [assignment: *the authorized identified roles*]
[210] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[211] [assignment: *list of TSF data*]
[212] [assignment: *the authorized identified roles*]

FMT_MTD.1.1/ eID-PIN_Unblock The TSF shall restrict the ability to unblock and change[213] the blocked eID-PIN[214] to

1. the ID_Card holder,
2. the Authentication Terminal (ATT) with the Terminal Authorization Level for eID-PIN management[215].

This item concerns the following application(s): eID.

301 *Application Note 69:* The unblocking procedure must be implemented according to [EACTR], sec. 3.5.2 and is relevant for the status as required by FIA_AFL.1/eID-PIN_\ Blocking. It can be triggered by either (i) the ID_Card holder being authenticated as required by FIA_UAU.1/PACE using the eID-PUK as the shared password or (ii) the ATT (FIA_UAU.1/Rightful_Terminal) proved the Terminal Authorization Level being sufficient for eID-PIN management (FDP_ACF.1/TRM).

302 FMT_MTD.1/eID-PIN_Activate Management of TSF data – Activating/Deactivating eID-PIN

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1.

FMT_MTD.1.1/ eID-PIN_Activate The TSF shall restrict the ability to activate and deactivate[216] the eID-PIN[217] to

the Authentication Terminal (ATT) with the Terminal Authorization Level for eID-PIN management[218].

This item concerns the following application(s): eID, eSign.

303 *Application Note 70:* The activating/deactivating procedures must be implemented according to [EACTR, sec. 3.5.2]. It can be triggered by the ATT (FIA_UAU.1/Rightful_Terminal) that proved a Terminal Authorization Level being sufficient for eID-PIN management (FDP_ACF.1/TRM).

304 FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data: fulfilled by FMT_MTD.1/ CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE

[213] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[214] [assignment: *list of TSF data*]
[215] [assignment: *the authorized identified roles*]
[216] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[217] [assignment: *list of TSF data*]
[218] [assignment: *the authorized identified roles*]

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol and the Terminal Access Control SFP[219].

Refinement: The certificate chain is valid if and only if

(1) the digital signature of the Terminal Certificate (C_T) has been verified as correct using the public key of the Document Verifier Certificate and the expiration date of the C_T is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate (C_{DV}) has been verified as correct using the public key in the Certificate of the Country Verifying Certification Authority (C_{CVCA}) and the expiration date of the C_{DV} is not before the Current Date of the TOE,

(3) the digital signature of the Certificate of the Country Verifying Certification Authority (C_{CVCA}) has been verified as correct using the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the C_{CVCA} is not before the Current Date of the TOE.

The static terminal public key (PK_{PCD}) contained in the C_T in a valid certificate chain is a secure value for the authentication reference data of a rightful terminal.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization Level[220] of a successful authenticated Service Provider (represented by a rightful terminal).

This item concerns the following application(s): ePassport, eID, eSign.

305 *Application Note 71:* The Terminal Authentication is used as required by FIA_UAU.1/ Rightful_Terminal and FIA_UAU.5. The Terminal Authorization Level derived from the C_{CVCA}, C_{DV} and C_T is used as TSF data for access control required by FDP_ACF.1/TRM.

306 The PP ([IDCARDPP]) also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. For the functional class FMT there are the following components:

SFR identifier	Comments
FMT_SMR.1/SSCD	concerns the following application(s): – eSign
FMT_SMF.1/SSCD	concerns the following application(s): – eSign
FMT_MOF.1/SSCD	concerns the following application(s):

[219] [assignment: *list of TSF data*]

[220] This certificate-calculated Terminal Authorisation Level can additionally be restricted by ID_Card holder at the terminal, s. [EACTR, part 3 C.4.2]. It is based on Certificate Holder Authorization Template (CHAT), see [EACTR, part 3 C.1.5]. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ID_Card holder’s restricting input at the terminal. This final CHAT reflects the effective authorization level, see [EACTR,part 3 C.4.2] and is then sent to the TOE by the command 'MSE:Set AT' within the Terminal Authentication (B.3 und B.11.1 of [EACTR, part 3]).

SFR identifier	Comments
	– eSign
FMT_MSA.1/Admin_SSCD	concerns the following application(s): – eSign
FMT_MSA.1/Signatory_SSCD	concerns the following application(s): – eSign
FMT_MSA.2/SSCD	concerns the following application(s): – eSign
FMT_MSA.3/SSCD	concerns the following application(s): – eSign
FMT_MSA.4/SSCD	concerns the following application(s): – eSign
FMT_MTD.1/Admin_SSCD	concerns the following application(s): – eSign
FMT_MTD.1/Signatory_SSCD	concerns the following application(s): – eSign eSign-PIN can be unblocked using the card-global eID-PUK. Although the PP allows using an additional eSign-specific eSign-PUK this is not implemented in the TOE.

307 FMT_SMR.1/SSCD Security roles

Hierarchical to: No other components.

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

FMT_SMR.1.1/ SSCD The TSF shall maintain the roles
R.Admin and R.Sigy[221].

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

308 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/SVD management, SCD operational,
4. Change the default value of the security attribute SCD Identifier,
5. *none*[222].

[221] [assignment: *the authorized identified roles*]

309 FMT_MOF.1/SSCD Management of security functions behaviour

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[223] the functions signature-creation function[224] to R.Sigy[225].

310 FMT_MSA.1/Admin_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/ SCD/SVD_Generation_SFP_SSCD,
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/SVD_Generation_SFP[226] to restrict the ability to modify[227] the security attributes SCD/SVD management[228] to R.Admin[229].

311 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_SSCD
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/ The TSF shall enforce the Signature-creation_SFP[230] to restrict the

[222] [assignment: *list of management functions to be provided by the TSF*]/[assignment: *list of other security management functions to be provided by the TSF*]

[223] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[224] [assignment: *list of functions*]

[225] [assignment: *the authorized identified roles*]

[226] [assignment: *access control SFP*(s), *information flow control SFP(s)*]

[227] [selection: *change_default, query, modify, delete*, [assignment: *other operations*]]

[228] [assignment: *list of security attributes*]

[229] [assignment: *the authorized identified roles*]

Signatory_SSCD	ability to modify[231] the security attributes SCD operational[232] to R.Sigy[233].

312 **FMT_MSA.2/SSCD** **Secure 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/SCD/SVD_Generation_SFP_SSCD,
FDP_ACC.1/Signature_Creation_SFP_SSCD
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/SVD Management and SCD operational[234].

313 Application Note 72: The security attribute for SCD/SVD Management ist set to “yes” for the user S.Admin and to “no” for the user S.Sigy. On the other hand 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.

314 **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/SVD Generation SFP, SVD Transfer SFP and Signature-creation SFP[235] to provide restrictive[236] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SSCD The TSF shall allow the R.Admin[237] to specify alternative initial values to override the default values when an object or information is created.

[230] [assignment: *access control SFP*(s), *information flow control SFP(s)*]
[231] [selection: *change_default, query, modify, delete*, [assignment: *other operations*]]
[232] [assignment: *list of security attributes*]
[233] [assignment: *the authorized identified roles*]
[234] [selection: *list of security attributes*]
[235] [assignment: *access control SFP*, information flow control SFP]
[236] [selection choose one of: *restrictive, permissive*, [assignment: *other property*]]
[237] [assignment: *the authorized identified roles*]

315 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/SVD_Generation_SFP_SSCD,
FDP_ACC.1/Signature_Creation_SFP_SSCD

FMT_MSA.4.1/SSCD The TSF shall use the following rules to set the value of security attributes:

1. If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation.
2. If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation[238].

316 *Application Note 73:* Because the TOE does not support SCD/SVD generation by the Signatory alone, the rule (2) is not relevant here.

317 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[239] the RAD[240] to R.Admin[241].

318 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/ The TSF shall restrict the ability to modify[242] the RAD[243] to R.Sigy[244].

[238] [assignment: *rules for setting the values of security attributes*]

[239] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[240] [assignment: *list of TSF data*]

[241] [assignment: *the authorized identified roles*]

[242] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

Signatory_SSCD

6.1.8 Class FPT Protection of the Security Functions

319 The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF-data. The security functional requirement FPT_EMS.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.

320 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution* [245] in excess of *non-useful information* [246] enabling access to

1. the Chip Authentication Private Key (SK_{PICC}),
2. the eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational)[247]
3. *none*[248]

and

4. the private Restricted Identification key SK_{ID},
5. the private signature key of the ID_Card holder (SCD; if the *eSign* is operational)[249].
6. *none*[250]

FPT_EMS.1.2 The TSF shall ensure any users[251] are unable to use the following interface ID_Card’s contactless interface and circuit contacts[252] to gain access to

[243] [assignment: *list of TSF data*]
[244] [assignment: *the authorized identified roles*]
[245] [assignment: *types of emissions*]
[246] [assignment: *specified limits*]
[247] [assignment: *list of types of TSF data*]
[248] [assignment: *list of types of (further) TSF data*]
[249] [assignment: *list of types of user data*]
[250] [assignment: *list of types of (further) user data*]
[251] [assignment: *type of users*]
[252] [assignment: *type of connection*]

1. the Chip Authentication Private Key (SK_{PICC}),
2. the eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational)[253]
3. *none*[254]

and

4. the private Restricted Identification key SK_{ID},
5. the private signature key of the ID_Card holder (SCD; if the *eSign* is operational)[255].
6. *none*[256].

This item concerns the following application(s): ePassport, eID, eSign.

321 *Application Note 74*: 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 ID_Card's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well.

322 FPT_FLS.1 Failure with preservation of secure state

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* [257].

This item concerns the following application(s): ePassport, eID, eSign.

323 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, peri-*

[253] [assignment: *list of types of TSF data*]

[254] [assignment: *list of types of (further) TSF data*]

[255] [assignment: *list of types of user data*]

[256] [assignment: *list of types of (further) user data*]

[257] [assignment: *list of types of failures in the TSF*]

odically during normal operation[258] to demonstrate the correct operation of the TSF[259].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[260].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[261].

This item concerns the following application(s): ePassport, eID, eSign.

324 *Application Note 75*: The ID_Card'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.

325 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[262] to the TSF[263] by responding automatically such that the SFRs are always enforced.

This item concerns the following application(s): ePassport, eID, eSign.

326 *Application Note 76*: The TO E 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.

327 The PP ([IDCARDPP]) also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. For the functional class FPT there are the following components:

SFR identifier	Comments

[258] [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*]]

[259] [selection: [assignment: *parts of TSF*], *the TSF*]

[260] [selection: [assignment: *parts of TSF*], *TSF data*]

[261] [selection: [assignment: *parts of TSF*], *TSF*]

[262] [assignment: *physical tampering scenarios*]

[263] [assignment: *list of TSF devices/elements*]

SFR identifier	Comments
FPT_EMS.1/SSCD	This SFR is covered by FPT_EMS.1 above. concerns the following application(s): – eSign
FPT_FLS.1/SSCD	This SFR is covered by FPT_FLS.1 above. concerns the following application(s): – eSign
FPT_PHP.1/SSCD	concerns the following application(s): – eSign
FPT_PHP.3/SSCD	This SFR is commensurate with FPT_PHP.3 above. concerns the following application(s): – eSign
FPT_TST.1/SSCD	This SFR is equivalent FPT_TST.1 above. concerns the following application(s): – eSign

328 **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

329 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 components:

- ALC_DVS.2 (Sufficiency of security measures),
- ATE_DPT.2 (Testing: security enforcing modules) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.Identification	OT.Personalization	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.SCD/SVD_Gen	OT.Sigy_SigF
FCS_CKM.1/DH_PACE			x	x	x								
FCS_CKM.1/DH_CA			x	x	x		x						
FCS_CKM.1/CA_PICC			x	x	x		x						
FCS_CKM.2/DH			x	x	x		x						
FCS_CKM.4			x	x	x								
FCS_COP.1/SHA			x	x	x		x						
FCS_COP.1/SIG_VER			x	x	x								
FCS_COP.1/AES					x								
FCS_COP.1/CMAC			x	x			x						
FCS_RND.1			x	x	x		x						
FIA_AFL.1/eID-PIN_Suspending		x	x	x	x								
FIA_AFL.1/eID-PIN_Blocking		x	x	x	x	x							
FIA_AFL.1/PACE						x							
FIA_API.1/CA			x	x	x		x						
FIA_UID.1/PACE			x	x	x								
FIA_UID.1/Rightful_Terminal		x	x	x	x								
FIA_UAU.1/PACE			x	x	x								
FIA_UAU.1/Rightful_Terminal		x	x	x	x								
FIA_UAU.1/SSCD												x	x
FIA_UAU.4			x	x	x								
FIA_UAU.5			x	x	x								
FIA_UAU.6			x	x	x								
FDP_ACC.1/TRM		x	x		x								
FDP_ACF.1/TRM		x	x		x								
FDP_RIP.1		x	x	x	x		x						
FTP_ITC.1/PACE						x							
FTP_ITC.1/CA			x	x	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					
FMT_LIM.2								x					
FMT_MTD.1/INI_ENA	x	x											
FMT_MTD.1/INI_DIS	x	x											

	OT.Identification	OT.Personalization	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.SCD/SVD_Gen	OT.Sigy_SigF
FMT_MTD.1/CVCA_INI			x	x	x								
FMT_MTD.1/CVCA_UPD			x	x	x								
FMT_MTD.1/DATE			x	x	x								
FMT_MTD.1/PA_UPD		x	x	x	x		x						
FMT_MTD.1/SK_PICC			x	x	x		x						
FMT_MTD.1/KEY_READ			x	x	x		x						
FMT_MTD.1/eID-PIN_Resume		x	x	x	x								
FMT_MTD.1/eID-PIN_Unblock		x	x	x	x								
FMT_MTD.1/eID-PIN_Activate		x	x	x	x								
FMT_MTD.3			x	x	x								
FPT_EMS.1									x				
FPT_FLS.1									x		x		
FPT_TST.1									x		x		
FPT_PHP.3			x						x	x			

Table 12: Coverage of Security Objectives for the TOE by SFR

331 For the coverage of security objectives derived from the SSCD Protection Profile by SFR this ST refers to [SSCDPP]. The rationale related to the security functional requirements from [SSCDPP] are exactly the same as given for the respective items of the security policy definitions in sec. 11.1 of [SSCDPP] and they are not conflicting to the coverage given in the Table 12 above.

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

333 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.

334 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 *eSign* application).
This property is covered by FDP_ACC.1/TRM and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorization level of a rightful terminal. This authorization level can be achieved by the terminal identification/authentication as required by the SFR

FIA_UID.1/Rightful_Terminal, FIA_UAU.1/Rightful_Terminal[264]. Since only an ATT can reach the necessary authorization level, using and management of eID-PIN (FIA_AFL.1/ eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking, FMT_MTD.1/eID-PIN_Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
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.
FMT_MTD.1/PA_UPD covers the related property of OT.Personalization (updating SO_C).
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

335 The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the Terminal- and the Chip Authentication, of these data exchanged (physical manipulation and unathorized modifying).
Physical manipulation is addressed by FPT_PHP.3.
Unathorized modifying of the stored data is addressed, in the first line, by FDP_ACC.1/TRM and FDP_ACF.1/TRM. A concrete authorization level is achieved by the terminal identification/authentication as required by the SFRs FIA_UID.1/ Rightful_Terminal, FIA_UAU.1/Rightful_Terminal (is supported by FCS_COP.1/ SIG_VER). The TA protocol uses the result of the PACE authentication (FIA_UID.1/ PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use eID-PIN as the shared secret, using and management of eID-PIN (FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking, FMT_MTD.1/eID-PIN_\ Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
To allow a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.
Unauthorized modifying of the exchanged data is addressed, in the first line, by FTP_\ ITC.1/CA using FCS_COP.1/CMAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication FIA_API.1/CA using FCS_CKM.1/DH_CA and possessing the special properties FIA_UAU.5, FIA_UAU.6. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/ SK_PICC governs creating/loading SK_{PICC}, which is generated conformant to [EACTR] as required by FCS_CKM.1/CA_PICC if the Chip Authentication Private Key is created, FMT_MTD.1/KEY_READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for K_{MAC}).
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalization Agent only and, hence, is to consider as trustworthily.
The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for

[264] which, in turn, are supported by the related FCS-components. The author of the PP dispensed here with listing of these supporting FCS-components for the sake of clearness. See the next item OT.Data_Integrity for further detail.

cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

336 The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF-data (after the Terminal- and the Chip Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.
This objective is mainly achieved by FTP_ITC.1/CA using FCS_COP.1/CMAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication FIA_API.1/CA using FCS_CKM.1/DH_CA and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC and FCS_CKM.1/ CA_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for K_{MAC}).
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalization Agent only and, hence, is to consider as trustworthily.
A prerequisite for successful CA is an accomplished TA as required by FIA_UID.1/ Rightful_Terminal, FIA_UAU.1/Rightful_Terminal (is supported by FCS_COP.1/SIG_\ VER). The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use eID-PIN as the shared secret, using and management of eID-PIN (FIA_AFL.1/ eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking, FMT_MTD.1/eID-PIN_ Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
To allow a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.
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.

337 The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the Terminal- and the Chip Authentication, of these data exchanged.
This objective for the data stored is mainly achieved by FDP_ACC.1/TRM and FDP_\ ACF.1/TRM. A concrete authorization level is achieved by the terminal identification/ authentication as required by the SFRs FIA_UID.1/Rightful_Terminal, FIA_UAU.1/ Rightful_Terminal (is supported by FCS_COP.1/SIG_VER). The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use eID-PIN as the shared secret, using and management of eID-PIN (FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_\ Blocking, FMT_MTD.1/eID-PIN_Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/ eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
To allow a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized

identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.
This objective for the data exchanged is mainly achieved by FTP_ITC.1/CA using FCS_COP.1/AES. A prerequisite for establishing this trusted channel is a successful Chip Authentication FIA_API.1/CA using FCS_CKM.1/DH_CA and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_\ PICC and FCS_CKM.1/CA_PICC governs creating/ loading SK_{PICC}, FMT_MTD.1/KEY_\ READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for K_{Enc}).
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalization Agent only and, hence, is to consider as trustworthily.
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.

338 The security objective **OT.ID_Card_Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the ID_Card remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ, eID-PIN, eID-PUK).
This objective is achieved as follows: (i) while establishing PACE communication with CAN, MRZ or eID-PUK (non-blocking authentication/authorization data) – by FIA_AFL.1/ PACE; (ii) while establishing PACE communication using eID-PIN (blocking authentication data) – by FIA_AFL.1/eID-PIN_Blocking; (iii) for listening to PACE communication and for establishing CA communication (if SO_C and PK_{PICC} are card-individual) – FTP_\ ITC.1/PACE; (iv) for listening to CA communication (readable and writable user data: document details data, biographic data, biometric reference data; eSign-PIN) – FTP_ITC.1/CA.

339 The security objective **OT.Chip_Auth_Proof** aims enabling verification of the authenticity of the TOE as a whole device.
This objective is mainly achieved by FIA_API.1/CA using FCS_CKM.1/DH_CA. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC and FCS_CKM.1/CA_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for CMAC).
The authentication token T_{PICC} is calculated using FCS_COP.1/CMAC. The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for cryptographic operations needed.
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalization Agent only and, hence, is to consider as trustworthily.

340 The security objective **OT.Prot_Abuse-Func** aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data.
This objective is achieved by FMT_LIM.1 and FMT_LIM.2 preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life phase.

341 The security objective **OT.Prot_Inf_Leak** aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE.

342 This objective is achieved

- by FPT_EMS.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 for forcing a malfunction of the TOE, and
- by FPT_PHP.3 for a physical manipulation of the TOE.

343 The security objective **OT.Prot_Phys-Tamper** aims protection of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE.
This objective is completely covered by FPT_PHP.3 in an obvious way.

344 The security objective **OT.Prot_Malfunction** aims ensuring a correct operation of the TOE by preventing its operation outside the normal operating conditions.
This objective is covered by FPT_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorized users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Rationale for SFR's Dependencies

345 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 analysed, and non-dissolved dependencies are appropriately explained.

346 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.1/DH_CA	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	FCS_CKM.2/DH FCS_CKM.4
3	FCS_CKM.1/CA_PICC	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	FCS_COP.1/AES, FCS_COP.1/CMAC FCS_CKM.4
4	FCS_CKM.2/DH	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA FCS_CKM.4
5	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA
6	FCS_COP.1/SHA	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	justification see page 51 FCS_CKM.4
7	FCS_COP.1/SIG_VER	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	justification see page 51 FCS_CKM.4

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
8	FCS_COP.1/AES	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA FCS_CKM.4
9	FCS_COP.1/CMAC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA FCS_CKM.4
10	FCS_RND.1	No dependencies	n.a.
11	FIA_AFL.1/eID-PIN_Suspending	FIA_UAU.1	FIA_UAU.1/PACE
12	FIA_AFL.1/eID-PIN_Blocking	FIA_UAU.1	FIA_UAU.1/PACE
13	FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1/PACE
14	FIA_API.1/CA	No dependencies	n.a.
15	FIA_UID.1/PACE	No dependencies	n.a.
16	FIA_UID.1/Rightful_Terminal	No dependencies	n.a.
17	FIA_UAU.1/PACE	FIA_UID.1	FIA_UID.1/PACE
18	FIA_UAU.1/Rightful_Terminal	FIA_UID.1	FIA_UID.1/Rightful_Terminal
19	FIA_UAU.4	No dependencies	n.a.
20	FIA_UAU.5	No dependencies	n.a.
21	FIA_UAU.6	No dependencies	n.a.
22	FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
23	FDP_ACF.1/TRM	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/TRM justification see page 65
24	FDP_RIP.1	No dependencies	n.a.
25	FTP_ITC.1/PACE	No dependencies	n.a.
26	FTP_ITC.1/CA	No dependencies	n.a.
27	FAU_SAS.1	No dependencies	n.a.
28	FMT_SMF.1	No dependencies	n.a.
29	FMT_SMR.1	FIA_UID.1	FIA_UID.1/PACE, FIA_UID.1/Rightful_Terminal see also Application Note 60
30	FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
31	FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
32	FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
33	FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
34	FMT_MTD.1/CVCA_INI	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
35	FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
36	FMT_MTD.1/DATE	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
37	FMT_MTD.1/PA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
38	FMT_MTD.1/SK_PICC	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
39	FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
40	FMT_MTD.1/eID-PIN_Resume	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
41	FMT_MTD.1/eID-PIN_Unblock	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
42	FMT_MTD.1/eID-PIN_Activate	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
43	FMT_MTD.3	FMT_MTD.1	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE
44	FPT_EMS.1	No dependencies	n.a.
45	FPT_FLS.1	No dependencies	n.a.
46	FPT_TST.1	No dependencies	n.a.
47	FPT_PHP.3	No dependencies	n.a.

Table 13: Dependencies between the SFRs

347 For the Justification of non-satisfied dependencies see the description of the corresponding SFRs in the chapter 6. 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.

348 The rationale for SFR's dependencies related to the security functional requirements taken over from [SSCDPP] are exactly the same as given for the respective items of the security policy definitions in sec. 6.2 loc. cit.

349 The table below shows the dependencies between the SFR of the TOE derived from the [SSCDPP]. SFRs which are equivalent to those from the [IDCARDPP] are not duplicated.

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

No.	SFR-component from the PP	Dependencies assumed	Fulfilled by SFR
50	FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD
51	FDP_ACC.1/Signature_Creation_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/Signature_Creation_SFP_SSCD
52	FDP_ACC.1/SVD_Transfer_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP_SSCD
53	FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD FMT_MSA.3/SSCD
54	FDP_ACF.1/Signature_Creation_SFP_SSCD	FDP_ACF.1 FMT_MSA.3	FDP_ACC.1/Signature_Creation_SFP_SSCD FMT_MSA.3/SSCD
55	FDP_ACF.1/SVD_Transfer_SFP_SSCD	FDP_ACF.1 FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP_SSCD FMT_MSA.3/SSCD
56	FDP_SDI.2/Persistent_SSCD	No dependencies	n.a.
57	FDP_SDI.2/DTBS_SSCD	No dependencies	n.a.
58	FIA_AFL.1/SSCD	FIA_UAU.1	FIA_UAU.1/SSCD
59	FIA_UAU.1/SSCD	FIA_UID.1	FIA_UID.1/SSCD
60	FIA_UID.1/SSCD	No dependencies	n.a.
61	FMT_MOF.1/SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1/SSCD
62	FMT_MSA.1/Admin_SSCD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD FMT_SMR.1/SSCD FMT_SMF.1/SSCD
63	FMT_MSA.1/Signatory_SSCD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Signature_Creation_SFP_SSCD FMT_SMR.1/SSCD FMT_SMF.1/SSCD
64	FMT_MSA.2/SSCD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD FMT_SMR.1/SSCD
65	FMT_MSA.3/SSCD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD FMT_SMR.1/SSCD
66	FMT_MSA.4/SSCD	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD FDP_ACC.1/Signature_Creation_SFP_SSCD
67	FMT_MTD.1/Admin_SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1/SSCD
68	FMT_MTD.1/Signatory_SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1/SSCD
69	FMT_SMF.1/SSCD	No dependencies	n.a.
70	FMT_SMR.1/SSCD	FIA_UID.1	FIA_UID.1/SSCD
71	FPT_PHP.1/SSCD	No dependencies	n.a.

Table 14: Dependencies between the SFRs required by [SSCDPP]

350 The dependency analysis shows that all dependencies being expected by CC part 2 and by extended components definition (chapter 5) are fulfilled.

6.3.3 Security Assurance Requirements Rationale

351 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.

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

353 The selection of the component ATE_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

354 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 ID_Card required by the ID_Card Issuer and reflected by the [IDCARDPP].

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

356 The augmentation of EAL4 chosen comprises the following assurance components ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package (cf. [IDCARDPP, Table 15]).

6.3.4 Security Requirements – Internal Consistency

357 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.

358 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.

359 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

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

361 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 ID_Card and the Service Provider connected
- Identification and authentication of users and components
- Audit
- Generation of the Signature Key Pair for the eSign application
- Creation of Digital Signatures by the eSign application
- Management of and access to TSF and TSF-data
- Accuracy of the TOE security functionality / Self-protection

362 They are already mentioned in section 6.1.1 and represent the functional description of the feature overview in section 1.4.2. 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

363 The access to User Data is restricted according to the SFRs FDP_ACC.1/TRM and FDP_ACF.1/TRM. Different types of Terminal (PCT, EIS, ATT and SGT) are assigned dedicated access rights after successful authentication protocol (cf. section 7.3) supported by FIA_UAU.1/PACE and FIA_UAU.1/Rightful_Terminal. For the eSign application the access to the signature creation data is additionally controlled by FDP_ACC.1/ Signature-creation_SFP_SSCD and FDP_ACF.1/Signature-creation_SFP_SSCD. 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).

7.2 Secure data exchange

364 The secure data exchange in a trusted channel is required by FTP_ITC.1/PACE and FTP_ITC.1/CA. 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, Terminal Authentication and the Chip Authentication governed by FIA_API.1/CA: Chip Identification/Authentication, and FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT). 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.

7.3 Identification and authentication of users and components

365 The identification and authentication protocol is decribed 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 users (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UID.1/SSCD, FIA_UIA.1/SSCD) and external entities like terminals of different types (FIA_UID.1/Rightful_Terminal, FIA_UAU.1/Rightful_Terminal). During the terminal authentication protocol a certificate is used, this is supported by FCS_COP.1/SIG_VER.

366 The TOE itself must also be authenticated, which is supported by FIA_API.1/CA. 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.

367 To prevent brute-force attacks the eID-PIN reference data will be suspended after consecutive failed authentication attempts, and will be blocked if a defined number of failed attempts is passed (FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking). Suspended reference data requires always the successful CAN authentication before any PIN authentication can be applied.

368 To prevent skimming attacks on non-blocking reference data, i. e. the CAN, MRZ and eID-PUK, the TOE blocks the authentication procedure after detecting any failed authentication attempt. Because the MRZ and the eID-PUK carry enough entropy this is even sufficient for a brute force attack which is not necessary for the CAN, because the latter is restricted revealable.

369 The identification and authentication of the ID_Card holder as Signatory, i.e. the intention of the User to create an electronic signature, requires the sucessful verification of a different eSign-PIN, which is usually a single one but may be also one of two. It is also a blocking if a dedicated number of consecutive failed attempts is passed (FIA_AFL.1/SSCD).

370 The security and the reliability of the identification and authentification is supported by the correct key agreement (FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA, FCS_CKM.2/DH, FCS_COP.1/SHA) and the quality of random numbers (FCS_RND.1) used by the ID_Card and the terminal. As the authentication state is left, the session keys can not be used anymore (FCS_CKM.4).

7.4 Audit

371 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 diabled for the Operational Phase (FMT_MTD.1/INI_DIS) by the Personalization Agent.

7.5 Generation of the *eSign* Signature Key Pair

372 The *eSign* Signature Key Pair is generated by the TOE (FCS_CKM.1/SSCD), such that the private key (SCD) does never appear outside the TOE and is destroyed if a new key is generated (FCS_CKM.4/SSCD).

373 The use of the SCD under access control (section 7.1), which is supported by FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD, and FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD.

374 The execution of the generation of a Signature Key Pair is accessible for the User S.Admin only, the initial Reference Authentication Data (RAD) is created (FMT_MTD.1/ Admin) but can never be used for signature creation. Only the User S.Sigy is able to change the RAD to an operational state (FMT_MSA.1/Signatory_SSCD, FMT_MSA.2/ SSCD).

375 The Signature Key Pair generation requires a secure channel to the User S.Admin, who receives through that channel also the Signature Verification Data (SVD). This is supported by FDP_ACC.1/SVD_Transfer_SFP_SSCD, FDP_ACF.1/SVD_Transfer_SFP_\ SSCD.

7.6 Creation of Digital Signatures

376 The creation of electronic signatures must fulfill the strong requirements of the Signature Law in Germany and the yearly issued by the Bundesnetzagentur List of Algorithms and Parameters ([ALGO]). The parameters for FCS_COP.1/SSCD are chosen in such a way that they fulfill these requirements also in the near future. Nevertheless the User S.Sigy is advised to follow the publications of the Bundesnetzagentur for the current status, otherwise the electronic signature may loose its status as *qualified* electronic signature.

7.7 Management of and access to TSF and TSF-data

377 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 Prepersonalization (FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). The during initialization necessary test features are no more availabe after TOE delivery (FMT_LIM.1, FMT_LIM.2).

378 After delivery the TOE is personalized (FMT_MTD.1/PA_UPD), the initial CVCA data is stored (FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE) together with the Chip Authentication Private Key (FMT_MTD.1/SK_PICC), which can only be used internally but never accessed else (FMT_MTD.1/KEY_READ). The Chip Authentication Private Key can be loaded on the TOE during Personalization (FMT_MTD.1/ SK_PICC) or generated (FCS_CKM.1/CA_PICC), following the same requirements as for ECDH ephemeral key agreement.

379 The eID-PIN can be resumed (FMT_MTD.1.1/eID-PIN-Resume) by the ID_Card holder after executing successfully the PACE protocol with the CAN and the e-ID-PIN itself. A blocked eID-PIN can be unblocked (FMT_MTD.1.1/eID-PIN-Unblock) by the ID_Card

holder or a Authentication Terminal with a corresponding authorization level. This is under access control (FDP_ACF.1/TRM) and supported by the certificate chain verification (FMT_MTD.3).

380 The eID-PIN can be activated and also deactivated (FMT_MTD.1.1/eID-PIN-Activate) by an Authentication Terminal with an authorization level sufficient for eID-PIN management. This is under access control (FDP_ACF.1/TRM) and supported by the certificate chain verification (FMT_MTD.3).

381 The eSign functionality is separately supervised by the operation system. All the access rules and the memory assignment is done during initialization phase and can not be changed later on, independent of the operational status of the application. The Administrator (Service Provider) can generate the SCD/SVD key pair (FMT_MSA.1/Admin_SSCD, FMT_MSA.3/SSCD, FMT_MSA.4/SSCD) and create the initial reference data objects (FMT_MSA.2/SSCD, FMT_MTD.1/Admin_SSCD).

382 Only the identified by the eID application User is able to set the SCD operational (FMT_MSA.2/SSCD, FMT_MSA.4/SSCD, FMT_MSA.1/Signatory_SSCD) and generate electronic signatures (FMT_MOF.1/SSCD, FMT_MTD.1/Signatory_SSCD).

7.8 Reliability of the TOE security functionality

383 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_EMS.1).

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

385 The TOE will permantly 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).

386 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).

387 This functionality is supported by the entire class FMT.

7.9 TOE SFR Statements

388 For the sake of completeness the TOE Summary Specification of the previous sections is re-ordered once again. All the TOE SFR statements are listed and it is described how they are fulfilled by the TOE. If appropriate requirements are handled together to avoid unneccessary text duplication.

389 FCS_CKM.1/DH_PACE: The EC Diffie-Hellman Session Key Derivation Algorithm uses a Challenge-Response-Protocol for the derivation of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

390 FCS_CKM.1/DH_CA: The EC Diffie-Hellman Session Key Derivation Algorithm uses a Challenge-Response-Protocol for the derivation of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

391 FCS_CKM.1/CA_PICC: The Chip Authentication Key Pair is usually loaded during Personalization. Beside this it can also be created by the TOE in this life cycle phase, but this is no more possible after the Personalization is finished.

392 FCS_CKM.2/DH: The keys used in the Diffie-Hellman key agreement are distributed by the means specified in the PACE protocol, which is proven to be secure and the standardized Chip Authentication protocol known to be a secure Challenge-Response-Protocol

393 FCS_CKM.4: Each session key is used only by the authenticated user and is destroyed if the authentication fails or is restarted again. Additionally in case of loss of power the keys are also erased, because they are not stored permanently.

394 FCS_COP.1/SHA: The hash function is used for key deriviation. The recently discovered collision attacks are not relevant for this application.

395 FCS_COP.1/SIG_VER uses the initial public key Country Verifying Certification Authority and the public keys in certificates provided by the terminals as TSF data for the Terminal Authentication Protocol and the Access Control. Their validity verified according to FMT_MDT.3 and their security attributes are managed by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. There is no need to import user data or manage their security attributes.

396 FCS_COP.1/AES: The AES algorithm is a generally recognized as secure encryption algorithm. No exploitable weakness is known, and the security level is higher than 100 bit, which is accepted as appropriate in the future.

397 FCS_COP.1/CMAC: The CMAC algorithm is a generally recognized as secure message authentication algorithm. This mode of operation fixes security deficiencies of the used before CBC-MAC.

398 FCS_RND.1: The randomness of values for challenges or ephemeral or permanent keys bases on the underlying hardware TSF. Its Random Number Generator claims the functionality class PTG.2 according to [AIS31]. This includes also the fulfillment of the online test requirements. For generating random nonces in the PACE protocol and the Terminal Authentication a cryptographic post-processing guarantees that statistical tests practically cannot distinguish between generated values and an ideal random number generator.

399 FCS_CKM.1/SSCD: The eSign key pair generation algorithm is compliant to the Technical Specification [ECCTR]. The available parameters can be chosen such that they are suitable for the near and the long future.

400 FCS_COP.1/SSCD: The cryptographic operation is implemented with care based on the knowledge and experience of T-Systems such that no leakage of secure user data can occur.

401 FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking and FIA_AFL.1/PACE implement well-known user authentication data handling. The feature of PIN suspending twarts the unwanted inconspicuous blocking. It is provided by the TOE based on the approved methods of ISO 7816 [ISO7816]. The ranges for the suspending value s_{ad} and the blocking value b_{ad} are defined in Administrator Guidance [TCOSADM]. They depend

on the length and the alphabet chosen for these PINs. The handling of non-blocking authentication data depends on its entropy. Whereas MRZ with random serial numbers and eID_PUK with at least 10 digits provide sufficient randomness, the CAN handling must be considered separately.

402 FIA_API.1/CA: The chip authentication implementation based on the description of the protocol in [EACTR] provides a proof of the authenticity of the chip, which is proven to prevent the Challenge Semantics attack. The private Chip Authentication is either leaded or created during personalization phase and can only be used after terminal authentication and never read out.

403 FIA_UID.1/PACE, FIA_UID.1/Rightful_Terminal FIA_UAU.1/PACE, FIA_UAU.1/Rightful_ Terminal, FIA_UAU.1/PACE, FIA_UAU.1/Rightful_Terminal, FIA_UAU.4: The access rules allow establishing a communication channel before the user is authenticated. After successful authentication of the Terminal based on PACE or Terminal Authentication Protocol a security status is maintained. Based on that status the access rules apply that allow or disallow the execution of commands and the access to security data controlled controlled by the Operating System of the TOE. The PACE protocol is proven to be secure.

404 FIA_UAU.5: The authentication of the Manufacturer, a Personalization Agent and a Terminal is controlled by the Access Rules laid down in the Operating System in a very early stage of the life cycle. Even if the file system is not available, the Initialization Data can only be written by a successfully authenticated user (in a Manufacturer’s role). The authentication attempts as Personalization Agent can be based on Symmetric Authentication Mechanism with the Personalization Agent Key and the Terminal Authentication Protocol with Personalization Agent Keys. The high entropy of the Symmetric Keys used herein guarantees the reliability of these authentications.
After run of the Terminal Authentication and the Chip Authentication Protocol the TOE accepts only commands with a correct message authentication code sent by means of Secure Messaging with key agreed with the terminal by means of the Chip Authentication Mechanism. The security proof of the protocol defined in [EACTR] guarantees the correctness and the reliability of the authentications.

405 FIA_UAU.6 The TOE guarantees based on the inherent MAC verification in the secure messaging mechanism that the re-authentication of the user or component (Personalization Agent, Terminal) is possible for every command after successful authentication.

406 FIA_UAU.1/SSCD: The Administrator (S.Admin) is authenticated by the Terminal Access Control. The successfully executed Terminal Authentication based on a certificate with a relative authorization “Install (qualified) certificate” according to [EACTR, Table C.4] authenticates the Administrator (CSP). The Signatory is authenticated based on the PACE Protocol and the sucessful ePIN verification, which is protected by the secure channel established before.

407 FIA_UID.1/SSCD: If the SCD/SVD is not generated yet, the default user will be identified as Administrator. If the SCD is set to “operational” then the default user is the Signatory. If the SCD is terminated (set to “not operational”) the default user will be again the Administrator (CSP). This behavior is determined by the access rules of the file system.

408 FIA_AFL.1/SSCD: Any failed authentication attempt will be detected by the TSF, and the consecutive authentication failures will be accumulated. Depending of the structure of the RAD the number sig_{ad} must be chosen from a specified in the Administrator Guidance range. The structure of RAD should be homogenous (nearly equally distributed) for the application of the table and the file system of the signature application must support

these restrictions. The User will be informed that the security of the authentication depends on the quality of the selected VAD/RAD. The file system of the TOE may be configured such that the RAD is set up of two pieces of data including the eSign-PIN each with its own retry counter. There is no local eSign-PUK foreseen, but the global eID-PUK can be used for resetting the signature authentication retry counter. A more detailed analysis covering that case is given in the Administrator Guidance ([TCOSADM]).

409 FDP_ACC.1/TRM The Terminal Access Control SFP access rules are fixed in the Operating System of the TOE; it can not be changed nor bypassed.

410 FDP_ACF.1/TRM The access control rules of FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE.

411 FDP_RIP.1: 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).

412 FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD: The execution of the generation of a Signature Key Pair is accessible for the User S.Admin only. The initial Reference Authentication Data (RAD) is created but can never be used for signature creation.

413 FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD: Access control rules of FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE.

414 FDP_ACC.1/SVD_Transfer_SFP_SSCD: The Signature Key Pair generation requires a secure channel to the User S.Admin, who receives through that channel also the Signature Verification Data (SVD), that will be used to issue a corresponding qualified certificate to the identified ID_Card holder.

415 FDP_ACF.1/SVD_Transfer_SFP_SSCD: The access control rules of FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE.

416 FDP_ACC.1/Signature_Creation_SFP_SSCD The use of the SCD is avaliable for the authenticated user only and is under access control (section 7.1). For authentication the entered VAD must coincide with the stored RAD.

417 FDP_ACF.1/ Signature_Creation_SFP_SSCD: The access control rules of FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE.

418 FDP_SDI.2/Persistent_SSCD, FDP_SDI.2/DTBS_SSCD: The stored User Data and the entered DTBS Data will be checked by the operating system for integrity errors, so any change will be detected. The user will be informed by the corresponding status code, that an error occurred. During opeartions the integrity check will be provided by the hardware.

419 FTP_ITC.1/PACE: The TOE provides a secured communication channel based on the approved algorithms of Secure Messaging if the PACE protocol with the selected authentication data.

420 FTP_ITC.1/CA: The TOE provides a secured communication channel based on the approved algorithms of Secure Messaging if the terminal has been authenticated as a rightful.

421 FAU_SAS.1: The IC Identification Data can be read by the successfully authenticated Manufacturer, which allows the Manufacturer to store this data in audit records. After Personalization the read access to IC Identification Data is disabled.

422 FMT_SMF.1, FMT_SMR.1: Maintaining the different roles and TSFs of the TOE using dedicated access rules can not be changed or disabled in the Operating System. The assignment of a specific role is supported by a successful authentication and the following-up Secure Messaging. The embedded software (i.e. the operating system) enforces the application of the access rules before any function is allowed to proceed.

423 FMT_LIM.1, FMT_LIM.2: Limitations of capabilities or availability are enforced by the Operating System of the TOE controlling the integrity of the stored access rules and the used functions. After Initialization all data testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use.

424 FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS: Initialization Data is used for audit log of a pre-personalized TOE. It is stored in the TOE, but the acces to this information is disabled as soon as the TOE is personalized.

425 FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE: The intial Personalization data from the Issuing Branch is

426 FMT_MTD.1/PA_UPD, FMT_MTD.1/SK_PICC: Only the User authenticated as Personalization Agent is able to update the Personalization Data and to create/load the private chip authentication key. These objects are under access control that is fixed in the file system and can never be changed in the operational phase.

427 FMT_MTD.1/KEY_READ: The private chip authentication key is object under access control that is fixed in the file system and can never be changed in the operational phase.

428 FMT_MTD.1/eID-PIN_Resume: Resuming a suspended eID-PIN requires the knowledge of the CAN and additionally the knowledge of the eID-PIN itself. The corresponding numbers of consecutive failed attempts can be selected from a defined in the Administrator Guidance interval, which is restricted by the security evaluation.

429 FMT_MTD.1/eID-PIN_Unblock: The eID-PIN can be unblock and re-initialized only by an Authentication Terminal that is granted a special authorization level.

430 FMT_MTD.1/eID-PIN_Activate: The eID-PIN can be activated and deactivated only by an Authentication Terminal that is granted a special authorization level.

431 FMT_MTD.3 The Operating System of the TOE accepts only valid certificates; this includes the existence of a valid certificate chain up to the trust anchor (CVCA key) of the TOE.

432 FMT_SMR.1/SSCD, FMT_SMF.1/SSCD: Maintaining the different roles and TSFs of the TOE using dedicated access rules can not be changed or disabled in the Operating System. The assignment of a specific role is supported by a successful authentication and the following-up Secure Messaging. The embedded software (i.e. the operating system) enforces the application of the access rules before any function is allowed to proceed.

433 FMT_MOF.1/SSCD: The User S.Admin creates the initial RAD, but can not set it to operational state. Only the Card_holder can access the initial RAD, change it and set it to the operational state.

434 FMT_MSA.1/Admin_SSCD, FMT_MSA.2/SSCD: The management of security attributes (FMT_MSA.1 and FMT_MSA.2) is under Access Control (section 7.1) that is fixed in the

file system and can never be changed in the personalization and operational phases. The attribute "authorized" for SCD/SVD Management is assigned only to the Administrator S.Admin (CSP) and this attribute can not be modified in the operational phase. During Personalization the attribute can only be set to "not authorized" for S.Admin in the operational phase but can never set to "authorized" for S.User. If in the operational phase the S.Admin is not authorized for SCD/SVD Management then the eSign application can not be activated later.

435 FMT_MSA.1/Signatory_SSCD, FMT_MSA.2/SSCD: The management of security attributes (FMT_MSA.1 and FMT_MSA.2) is under Access Control (section 7.1) that is fixed in the file system and can never be changed in the operational phase. The attribute "operational" for SCD can be set or removed (set to "not operational") only by the Signatory S.Sigy.

436 FMT_MSA.3/SSCD: In the file system the initial values for the security attributes "authorized" for SCD/SVD Management and "operational" for SCD are set restrictive according to the corresponding SFPs. The Signatory S.Sigy is not allowed to generate .the SCD/SVD pair and the CSP (S.Admin) can never set the SCD "operational".

437 FMT_MSA.4/SSCD: Because the TOE does not support SCD/SVD generation by the Signatory, and because S.Admin and S.Sigy are different entities, there is no single operation that generates SCD/SVD pair and sets at the same time the SCD "operational".

438 FMT_MTD.1/Admin_SSCD: The initial RAD (reference authentication data) is generated by the CSP (S.Admin). This special RAD value (PIN in transport mode) can never be used for creating digital signatures.

439 FMT_MTD.1/Signatory_SSCD: Only the Signatory, authenticated as the ID_Card holder can modify the initial RAD (PIN in transport mode). After the initial RAD value is changed by the Signatory, the SCD can be set to "operational".

440 FPT_EMS.1: The Operating System of the TOE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication is closed. The strict care of uniformity and non-overloading single components is implemented in the Operating System and will be described detailed in ADV and AVA documentation. This implies the leakage of information about the Personalization Agent Authentication Key and the Chip Authentication Key.

441 FPT_FLS.1: The Operating System of the TOE guarantees that the TOE preserves a secure state if a test failure or integrity check mismatch occur

442 FPT_TST.1: The self tests of the underlying hardware and additional test maintained by the TOE provide the means for demonstrating that the TSF operation is correct and that the data is not manipulated.

443 FPT_PHP.3: The Operating System of the TOE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication will be closed immediately.

444 FPT_PHP.1/SSCD: The Operating System monitors the regular execution of commands and follows the information given by the hardware security functions. If physical tampering is detected by the hardware the communication will be closed immediately and the TOE enters a secure state.

7.10 Statement of Compatibility

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

7.10.1 Relevance of Hardware TSFs

446 In the following lists the relevance of the hardware security services (SS) and functions (SF) for the composite security target is considered.

447 **Relevant:**

- SS.RNG: Random Number Generator
- SS.HW_DES: Triple-DES Co-processor
- SS.HW_AES: AES Co-processor
- SS.CRC: Cyclic Redundancy Check
- SF.OPC: Control of Operating Conditions
- SF.PHY: Protection against Physical Manipulation
- SF.LOG: Logical Protection
- SF.SFR_ACC: Special Function Register Access Control
- SF.MEM_ACC: Memory Access Control

448 Note that the DES algorithm of the Security Service SS.HW_DES is used by the TOE in the algorithmic post-processing of the Random Number Generator. Nevertheless the Triple DES TDES is not used which implies that the reletated Security Objectives are not relevant (cf. 115).

449 **Not relevant:**

- SS.RECONFIG: Customer Reconfiguration
- SF.COMP: Protection of Mode Control
- SF.FFW: Firmware Firewall
- SF.FIRMWARE: Firmware Support

7.10.2 Security Requirements

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

451 **Security Requirements of the TOE related to the Composite ST:**

452 The following Security Requirements of the TOE are specific for the Applications of the Identity Card and have no conflicts with the underlying hardware.

FCS_CKM.1/DH_PACE	not relevant
FCS_CKM.1/DH_CA	not relevant
FCS_CKM.1/CA_PICC	not relevant
FCS_CKM.2/DH	not relevant
FCS_CKM.4	no conflicts
FCS_COP.1/SHA	not relevant
FCS_COP.1/SIG_VER	not relevant
FCS_COP.1/CMAC	no conflicts
FIA_AFL.1/eID-PIN_Suspending	no conflicts
FIA_AFL.1/eID-PIN_Blocking	no conflicts
FIA_AFL.1/PACE	no conflicts
FIA_API.1/CA	no conflicts
FIA_UID.1/PACE	no conflicts
FIA_UID.1/Rightful_Terminal	no conflicts
FIA_UAU.1/PACE	no conflicts
FIA_UAU.1/Rightful_Terminal	no conflicts
FIA_UAU.4	no conflicts
FIA_UAU.5	no conflicts
FIA_UAU.6	no conflicts
FIA_UAU.1/SSCD	no conflicts
FDP_ACC.1/TRM	not relevant
FDP_ACF.1/TRM	not relevant
FDP_RIP.1	no conflicts
FTP_ITC.1/PACE	not relevant
FTP_ITC.1/CA	not relevant
FMT_SMF.1	no conflicts
FMT_SMR.1	not relevant
FMT_MTD.1/INI_ENA	not relevant
FMT_MTD.1/INI_DIS	not relevant
FMT_MTD.1/CVCA_INI	not relevant
FMT_MTD.1/CVCA_UPD	not relevant
FMT_MTD.1/DATE	not relevant
FMT_MTD.1/PA_UPD	not relevant
FMT_MTD.1/SK_PICC	not relevant
FMT_MTD.1/KEY_READ	not relevant
FMT_MTD.1/eID-PIN_Resume	not relevant
FMT_MTD.1/eID-PIN_Unblock	not relevant
FMT_MTD.1/eID-PIN_Activate	not relevant
FMT_MTD.3	not relevant
FPT_TST.1	no conflicts

453 Note that some of these requirements, e.g., FCS_CKM.1/DH_PACE rely also on requirements of the hardware as FCS_RNG.1 [HW]. Nevertheless it is considered as not relevant, because the latter is already covered by FCS_RND.1 of the TOE.

454 The remaining Security Requirements of the TOE can be mapped to Security Requirements of the hardware. They show no conflict between each other.

FCS_COP.1/AES	matches FCS_COP.1[HW_AES] of [HWST]
FCS_RND.1	matches FCS_RNG.1[HW] of [HWST]
FAU_SAS.1	matches FAU_SAS.1[HW] of [HWST]
FMT_LIM.1	matches FMT_LIM.1 of [HWST]
FMT_LIM.2	matches FMT_LIM.2 of [HWST]
FPT_EMS.1	is supported by the Security Feature SF.OPC of the hardware ([HWST]) and the AVA_VAN.5 evaluation
FPT_FLS.1	matches FPT_FLS.1 of [HWST]
FPT_PHP.3	matches FPT_PHP.3 of [HWST]

455 Security Requirements of the hardware

- FAU_SAS.1[HW] covered by FAU SAS.1 of the Composite ST
- FCS_COP.1[HW_AES] covered by FCS_COP.1/AES of the Composite ST
- FCS_COP.1[HW_DES] not relevant, TDES is not used in the OS
- FCS_RNG.1[HW] matches FCS_RND.1 of the Composite ST
- FDP_ACC.1 [MEM] and [SFR] (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 [MEM] and [SFR] (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[HW] (Basic internal transfer protection) is covered by FPT_EMS.1 of the Composite ST
- FDP_IFC.1 (Subset information flow control) is covered by FPT_EMS.1 of the Composite ST
- FMT_SMF.1[HW] (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 [MEM] and [SFR] (Management of security attributes) no conflicts
- FMT_MSA.3 [MEM] and [SFR] (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[HW] (Basic internal TSF data transfer protection) is covered by FPT_EMS.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 STFDP_SDI.2[HW] (Stored data integrity monitoring and action) concerns the hardware operation, does not conflict with SFRs of the TOE

456 **FRU_FLT.2 (Limited fault tolerance) concerns the hardware operation, does not conflict with SFRs of the TOESecurity Assurance Requirements**

457 The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

458 The chosen level of assurance of the hardware is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2. This includes ALC_DVS.2, ATE_DPT.3 and AVA_VAN.5.

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

7.10.3 Security Objectives

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

461 **Security Objectives of the TOE related to the Composite ST:**

- OT.Data_Integrity covers O.HW_AES of the [HWST]
- OT.Data_Authenticity covers O.HW_AES of the [HWST]
- OT.Data_Confidentiality covers O.HW_AES of the [HWST]
- OT.ID_Card_Tracing no conflict
- OT.Chip_Auth_Proof no conflict
- OT.Prot_Abuse-Func covers O.Prot_ Abuse-Func from [PP0035]
- OT.Prot_Inf_Leak covers O.Leak-Inherent and O.Leak-Forced from [PP0035]
- OT.Prot_Phys-Tamper covers O.Phys-Probing and O.Phys-Manipulation from [PP0035]
- OT.Prot_Malfuntion matches O.Prot_Malfuntion from [PP0035]
- OT.Identification matches O.Identification from [PP0035]
- OT.Personalization no conflict

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

- O.Leak-Inherent (Protection against Inherent Information Leakage) is covered by OT.Prot_Inf_Leak
- O.Phys-Probing (Protection against Physical Probing) is mapped to OT.Prot_Phys-Tamper
- O.Malfunction (Protection against Malfunctions) is covered by the corresponding objective OT.Malfunction
- O.Phys-Manipulation (Protection against Physical Manipulation) is mapped to OT.Prot_Phys-Tamper
- O.Leak-Forced (Protection against Forced Information Leakage) is covered by OT.Prot_Inf_Leak

- O.Abuse-Func (Protection against Abuse of Functionality) is covered by the corresponding objective OT. Abuse-Func
- 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.INTEGRITY_CHK: Integrity control of transferred data

  The hardware provides a security service for stored data integrity checks and an operation control feature for data transfer, both used by the TOE. As it concerns the hardware reliability it is mapped to OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.
- O.HW_DES3 (Triple DES Functionality) not relevant

  The TDES functionality is not used in TOE's OS, therefore related objectives must not be considered.
- O.HW_AES (AES Functionality) is mapped to OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality.

  The AES Functionality is used to ensure the integrity and the confidentiality of personal data during transmission
- O.CUST_RECONFIG: Customer Option Reconfiguration (not relevant)

  This functionality is not used in TOE's OS.
- O.EEPROM_INTEGRITY: Integrity support of data stored in EEPROM

  The hardware shall provide a mechanism to support the integrity of the data stored in the EEPROM. This objective is mapped due to the used in hardware security features to OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.
- O.FM_FW: Firmware Mode Firewall (not relevant)

  This functionality is not used in TOE's OS.
- O.MEM_ACCESS is mapped to OT.Prot_Abuse-Func

  This objective for the hardware supports the correct operation of the TOE providing memory area access control.
- O.SFR_ACCESS is mapped to OT.Prot_Abuse-Func

  The objectives O.MEM_ACCESS and O.SFR_ACCESS support the correct operation of the TOE providing memory area access and Special Function Registers access control. Therefore these objectives are mapped to OT.Prot_Abuse-Func.

463 **Security Objectives for the eSign application ([SSCDPP]):**

- OT.Lifecycle_Security is covered by OT.Data_Integrity, OT.Data_Authenticity, and OT.Data_Confidentiality. The explicit mentioned in [SSCDPP] functionality of SCD destruction is supported by FCS_CKM.4

- OT.SCD/SVD_Gen is mapped to OT.Data_Authenticity, only a authorized user can invoke the SCD/SVD Generation
- OT.SCD_Unique is mapped to O.RND of the hardware ST and to OT.Data_ Authenticity and OT.Data_Confidentiality of the Composite ST
- OT.SCD_SVD_Corresp no conflicts

  The proof of correspondence between an SCD stored in the TOE and an SVD is implicit in the security mechanisms applied by the CGA.
- OT.SCD_Secrecy is covered by OT.Data_Confidentiality, OT.Prot_Inf_Leak and OT.Phys_Tamper.
- OT.Sig_Secure The use of robust technology is covered by OE.Legislative_Compliance, e.g. by the support of the signature algorithm specification ([ALGO]).
- OT.Sigy_SigF is covered by OT.Data_Authenticity
- OT.DTBS_Integrity_TOE is covered by OT.Data_Integrity
- OT.EMS_Design is covered by OT.Prot_Inf_Leak and OT.Phys_Tamper
- OT.Tamper_ID is covered by OT.Phys_Tamper
- OT.Tamper_Resistance is covered by OT.Phys_Tamper

- OE.CGA_QCert is mapped to OE.Legislative_Compliance, OE.Terminal_\ Authentication and OE.Terminal, only rightful CSPs are allowed to issue qualified certificates
- OE.SVD_Auth is covered by OT.Data_Integrity and is mapped to OE.Legislative_Compliance, OE.Terminal_Authentication and OE.Terminal for the environment
- OE.SSCD_Prov_Service is covered by objective for the ID_Card issuer: OE.Legislative_Compliance
- OE.HID_VAD is covered by OT.Data_Integrity, OT.Data_Confidentiality and OE.Terminal_Authentication and OE.Terminal for the environment
- OE.DTBS_Intend is covered by OE.ID_Card-Holder
- OE.DTBS_Protect is covered by OE.ID_Card-Holder and OE.Terminal
- OE.Signatory is covered by OE.ID_Card-Holder

  The obligation for a CSP activating an eSign application is to supply the ID_card holder as Signatory with the necessary User Guidance documentation according P.CSP_QCert. The TCOS Adminstrator Guidance ([TCOSADM]) provides further details what shall be included in the eSign User Guidance.

7.10.4 Compatibility: TOE Security Environment

464 Assumptions

465 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.

466 Assumptions for the TOE related to the Composite ST:

467 There are no additional assumptions besides the following ones.

468 Assumptions of the SSCD PP ([SSCDPP]):

- A.CGA is covered by the Security Objectives for the TOE Environment OE.CGA_QCert and OE.SVD_Auth required by the [SSCDPP].
- A.SCA is covered by the Security Objectives for the TOE Environment OE.DTBS_Intend required by the [SSCDPP].

469 The identified here Objectives are related to OE.Passive_Auth_Sign and OE.Personalization, that ensure the establishment of the correct identity of the eID_Card holder before the eSign application is activated. Note that authentic SVD for a certificate may be created already during Personalization as long as the corresponding secret key remains unknown and unusable until the eID_Card holder engage a CSP to make it available after certificate creation.

470 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_Authenticity, OT.Data_Confidentiality and TOE's Environment Objective OE.Chip_Auth_Key.

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

- A.Check-Init (Check of Initialization Data by the Security IC Embedded Software)

  The Check of Initialization Data of the hardware is related to the Life Cycle Phase 2 “Manufacturing of the TOE” and should not be confused with the check of Initialization Data during Personalization. The Assumption A.Check-Init is no more relevant after TOE Initialization, because Hardware Initialization Data is overridden by TOE's Initialization and Pre-Personalization Data.
- A.Key-Function (Usage of Key-dependent Functions)

  This assumption requires that key-dependent functions are implemented in the OS such that they are not susceptible to leakage attacks. It is covered by the Hardware‘s objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 “Development”.

472 Threats

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

474 Threats for the TOE related to the Composite ST:

- T.Skimming no conflict
- T.Eavesdropping no conflict
- T.ID_Card_Tracing no conflict
- T.Forgery covers T.RND of the Smardcard IC PP [PP0035]
- T.Counterfeit no conflict
- T.Abuse-Func matches the corresponding threat of the of the Smardcard IC PP [PP0035]
- T.Information_Leakage matches T.Leak-Inherent and T.Leak-Forced of the Smardcard IC PP [PP0035]
- T.Phys-Tamper matches T.Phys-Probing and T.Phys-Manipulation of the Smardcard IC PP [PP0035]
- T.Malfunction matches corresponding threat of the Smardcard IC PP [PP0035]

475 Threats of the hardware ST related to PP0035:

- T.Leak-Inherent matches T.Information_Leakage of the Composite ST
- T.Phys-Probing matches T.Phys-Tamper of the Composite ST
- T.Malfunction matches corresponding threat of the Composite ST
- T.Phys-Manipulation matches T.Phys-Tamper of the Composite ST
- T.Leak-Forced matches T.Information_Leakage of the Composite ST
- T.Abuse-Func matches corresponding threat of the Composite ST
- T.RND is covered by T.Information_Leakage and T.Forgery of the Composite ST and T.SCD_Divulg of the SSCD PP [SSCDPP]

  This threat (Deficiency of Random Numbers) is covered by T.Information_Leakage and T.Forgery because the Random Number Generator is used by the TOE for key generation and User Data protection. In case the key data is disclosed the confidentiality and integrity protection fails (for the actual session or Chip authentication). The same applies for SCD Generation if the eSign Application becomes operational.

476 Threats of the hardware ST ([HWST]):

- T.Unauthorised_Access Unauthorised Memory or Hardware Access

  This threat is related to the partitioning of memory areas in Boot Mode, Firmware Mode, System Mode and segmentation of memory areas in User Mode. This threat is covered by the objectives O.FW_HW, O.MEM_ACCESS, and

O.SFR_ACCESS of the Hardware ([HWST]] and may be considered as part of the threat T.Abuse-Func of the Protection Profile [IDCARDPP].

477 **Threats of the of the SSCD PP ([SSCDPP]):**

- T.SCD_Divulg is covered by T.Information_Leakage and T.Forgery of the Composite ST
- T.SCD_Derive is covered by T.Information_Leakage
- T.Hack_Phys matches T.Phys-Tamper of the Composite ST
- T.SVD_Forgery is covered by T.Forgery of the Composite ST
- T.SigF_Misuse is covered by T.Malfunction and T.Abuse-Func of the Composite ST
- T.DTBS_Forgery is covered by T. Forgery of the Composite ST
- T.Sig_Forgery is covered by T.Malfunction and T.Abuse-Func of the Composite ST

7.10.5 Organizational Security Policies

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

479 **Organizational Security Policies of the Composite ST of the TOE:**

P.Pre-Operational	covers P.Process-TOE of the hardware ST
P.Terminal	no conflict
P.ID_Card_PKI	no conflict
P.Terminal_PKI	no conflict
P.Trustworthy_PKI	no conflict

480 **Organizational Security Policies of the Hardware ST:**

- P.Add-Components (Additional Specific Security Components) no conflict

  The TOE’s hardware provides AES encryption/decryption and Area based Memory Access Control, Memory separation for different software parts and Special Function Register Access Control as security functionalities to the Security IC Embedded Software.
  They are used in security functionalities of the TOE and are considered in the implementation of the OS. The TOE’s hardware provides also Triple-DES encryption and decryption, which is not used in the OS.
- P.Process-TOE ([PP0035]) is covered by P.Pre-Operational of the Composite ST

481 **Organizational Security Policies of the of the SSCD PP ([SSCDPP]):**

P.CSP_QCert	no conflict
P.QSign	no conflict
P.Sigy_SSCD	no conflict
P.Sig_Non-Repud	no conflict

7.10.6 Conclusion

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

7.11 Assurance Measures

483 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 eID_Card
	ADV_FSP.4	Functional Specification TCOS eID_Card
	ADV_IMP.1	Implementation of the TSF TCOS eID_Card
	ADV_TDS.3	Modular Design of TCOS eID_Card
Guidance documents		
	AGD_OPE.1	User Guidance TCOS eID_Card
	AGD_PRE.1	Administrator Guidance TCOS eID_Card
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 eID_Card
	ALC_TAT.1, ALC_DVS.2	Development Tools and Development Security for TCOS eID_Card
Tests		
	ATE_COV.2, ATE_DPT.2	Test Documentation for TCOS eID_Card
	ATE_FUN.1	Test Documentation of the Functional Testing
Vulnerability assessment		
	AVA_VAN.5	Independent Vulnerability Analysis TCOS eID_Card

484 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.

485 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.

486 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.

487 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.

488 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 Enterprise Services GmbH.

489 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

490 This is the unchanged chapter from [IDCARDPP], more detailed information can be found there, too.

Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the ID_Card's chip to produce Terminal Certificates with the correct certificate effective date, see also [EACTR], sec. 2.2.5].
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 ID_Card's chip to store the Initialization Data and Pre-personalization Data.
Authentication terminal (ATT)	A technical system being operated and used either by a governmental organization (Official Domestic Document Verifier) or by any other, also commercial organization and (i) verifying the ID_Card presenter as the ID_Card holder (using the secret eID-PIN[265]), (ii) updating a subset of data of the eID application and (iii) activating the eSign application. See also [EACTR], chap. 3.2 and C.4.
Authenticity	Ability to confirm that the ID_Card itself and the data elements stored in were issued by the ID_Card 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.
Basic Inspection System (BIS)	A technical system being used by an authority[266] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying correspondence between the stored and printed MRZ. BIS implements the terminal's part of the Basic Access Control protocol and authenticates itself to the ID_Card using the Document Basic Access Keys drawn from printed MRZ data for reading the less-sensitive data (ID_Card document details data and biographical data) stored on the ID_Card (ePassport application only). See also [EACTR], chap. G.1 and H; also [ICAO9303-1].
Biographical data (biodata)	The personalized details of the ID_Card holder appearing as text in the visual and machine readable zones of and electronically stored in the ID_Card. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the ID_Card holder in the ID_Card as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed

[265] the secret eID-PUK can be used for unblocking the eID-PIN and resetting the retry counter related

[266] concretely, by a control officer

Term	Definition
	on a label on the Identification Card) or dynamic (randomly chosen by the electronic ID_Card and displayed by it using e.g. ePaper, OLED or similar technologies), see [EACTR], sec. 3.3
Card Security Object (SO_C)	A RFC 3369 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the ID_Card (EF.CardSecurity, see [EACTR], Table A.1 and sec. A.1.2) and carries the hash values of different Data Groups as defined in [EACTR], Appendix A. It shall also carry the Document Signer Certificate (C_{DS}) [EACTR], A.1.2.
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].
Country Signing CertA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the ID_Card Issuer with respect to confirming correctness of user and TSF data stored in the ID_Card. The CSCA represents the country specific root of the PKI for the ID_Cards and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed Country Signing CertA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [ICAO9303-1], 5.1.1. The Country Signing CertA issuing certificates for Document Signers (cf. [ICAO9303-1]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [EACTR], sec. 2.2.1
Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the ID_Card Issuer with respect to protection of user data stored in the ID_Card (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the rightful terminals (EIS, ATT, SGT) and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EACTR], chap. 2.2.1. The CSCA issuing certificates for Document Signers (cf. [ICAO9303-1]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [EACTR], sec. 2.2.1
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.
Document Details Data	Data printed on and electronically stored in the ID_Card representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the ePassport application of the ID_Card. It may carry the Document Signer Certificate (C_{DS}); see [ICAO9303-1]
Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the ID_Card Security Object stored on the ID_Card for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR], chap. 1.1 and [ICAO9303-1]. This role is usually delegated to the Personalization Agent.
Document Verifier (DV)	An organization (certification authority) enforcing the policies of the CVCA and of a service provider (governmental or commercial organization) and managing the terminals belonging together (e.g. terminals operated by a State's border police) by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a CertA, authorized by at least the national CVCA to issue certificates for national terminals, see [EACTR], chap. 2.2.2.

Term	**Definition**
	There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ID_Card Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (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[267]).
Eavesdropper	A threat agent reading the communication between the ID_Card and the Service Provider to gain the data on the ID_Card.
eID application	A part of the TOE containing the non-executable, related user data and the data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application. See [EACTR], sec. 3.1.2
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO9303-1]
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [EACTR], sec. 3.1.1.
eSign application	A part of the TOE containing the non-executable data needed for generating advanced or qualified electronic signatures on behalf of the ID_Card Holder as well as for authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified digital signature of the ID_Card Holder is required. The eSign application is optional: it means that it can optionally be activated[268] on the ID_Card by a Certification Service (or on his behalf) using the ATT with an appropriate authorization level. See [EACTR], sec. 3.1.3.
Extended Access Control	Security mechanism identified in [ICAO9303-1] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System (EIS)	See *Inspection system*
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]
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.
ID_Card (electronic)	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally)
ID_Card holder	The rightful/legitimated holder of the electronic ID Card for whom the issuing authority personalized the ID Card.
ID_Card Issuer (issuing authority)	Organization authorized to issue an electronic Identity Card to the ID_Card holder
ID_Card presenter	A person presenting the ID_Card to a terminal and claiming the identity of the ID_Card holder.

[267] Existing 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.

[268] 'activated' means (i) generate and store in the *eSign* application one or more signature key pairs and (ii) optionally store there the related certificates

Term	**Definition**
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]
Initialisation Data	Any data defined by the ID_Card 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).
Inspection	The act of an authority examining an ID_Card presented to it by an ID_Card presenter and verifying its authenticity as the ID_Card holder. See also [ICAO9303-1].
Inspection system (EIS)	A technical system being used by an authority[269] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ID_Card presenter as the ID_Card holder (for *ePassport*: by comparing the real biometrical data of the ID_Card presenter with the stored biometrical data of the ID_Card holder). The specification [EACTR], sec. 3.2 (and C.4) knows only one type of the inspection system, namely according to the result of the terminal authentication in the context of the Extended Access Control. It means that the Inspection System in the context of [EACTR], (and of the PP IDCARDPP) is commensurate with the Extended Inspection System (EIS) as defined in [EACPP3.1][270].
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The ID_Card's chip is an integrated circuit.
Integrity	Ability to confirm the ID_Card and its data elements stored upon have not been altered from that created by the ID_Card 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]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO9303-1]. The capacity expansion technology used is the MRTD's chip.
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]
Malicious equipment	A technical device does not possessing a valid, certified key pair for its authentication; validity of its certificate is not verifiable up to the respective root CertA (CVCA for a terminal and CSCA for an ID_Card).
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the ID_Card Manufacturer completing the IC to the ID_Card. 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 ID_Card Manufacturer using this role Manufacturer.

[269] concretely, by a control officer

[270] please note that an Extended Inspection System also covers the General Inspection Systems (GIS) in the sense of [EACPP3.1]

Term	**Definition**
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 Authorisation 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 ID_Card using a shared password (CAN, eID-PIN, eID-PUK or MRZ). 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.
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 ID_Card holder. PIN is a blocking password, see [EACTR], sec. 3.3
Personalization	The process by which the individual-related data (biographic and biometric data, signature key pair(s) for the eSign application) of the ID_Card holder are stored in and unambiguously, inseparably associated with the ID_Card.
Personalization Agent	An organization acting on behalf of the ID_Card Issuer to personalize the ID_Card for the ID_Card holder by some or all of the following activities: (i) establishing the identity of the ID_Card holder for the biographic data in the ID_Card[271], (ii) enrolling the biometric reference data of the ID_Card holder[272], (iii) writing a subset of these data on the physical Identification Card (optical personalization) and storing them in the ID_Card (electronic personalization) for the ID_Card holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card Security Object defined in [ICAO9303-1] (in the role of DS). A Personalization Agent acts, amongst other, as the Document Signer (item (vi) of his tasks). Generating signature key pair(s) is not in the scope of the tasks of this role, but the Personalization Agent may support a CSP actions providing Personalization Data to the CSP.
PIN Unblock Key (PUK)	A long secret password being only known to the ID_Card holder. The PUK is a non-blocking password, see [EACTR], sec. 3.3
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 ID_Card and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalized ID_Card's chip	ID_Card's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Receiving State	The Country to which the ID_Card holder is applying for entry. [ICAO9303-1]
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.
Remote terminal	A remote device directly communicating with the TOE and using the technical infrastructure between them (Internet, a local RF-terminal) merely as a message carrier. Only after Chip Authentication when a secure end-to-end connection between the TOE and remote terminal is established, the TOE grants access to the data of the eID application, see [EACTR], sec. 3.4.1

[271] relevant for the ePassport, the eID and the eSign applications

[272] relevant for the ePassport application

Term	**Definition**
Restricted Identification	Restricted Identification aims providing a temporary ID_Card identifier being specific for a terminal sector (pseudo-anonymization) and supporting revocation features (sec. 2.3, 4.1.2, 4.5 of [EACTR]. The security status of ID_Card is not affected by Restricted Identification.
Rightful equipment (rightful terminal or rightful ID_Card)	A technical device possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either EIS or ATT or SGT. A terminal as well as an ID_Card can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for an ID_Card – CSCA.
Secondary image	A repeat image of the holder’s portrait reproduced elsewhere in the document by whatever means. [ICAO9303-1]
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 ID_Card holder. Service Provider uses the rightful terminals managed by a DV.
Signature terminal (SGT)	A technical system being used for generation of digital signatures. See [EACTR], chap. 3.2 and C.4. It is equivalent – as a general term – to SCA and HID as defined in [SSCDPP].
Skimming	Imitation of a rightful terminal to read the ID_Card or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ CAN, eID-PIN or eID-PUK data.
Terminal	A technical system communicating with the TOE through the contactless interface. The role ‘Terminal’ is the default role for any terminal being recognized by the TOE as neither PCT nor EIS nor ATT nor SGT (‘Terminal’ is used by the ID_Card presenter).
Terminal Authorization Level	Intersection of the Certificate Holder Authorizations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the ID_Card gathered by inconspicuous (for the ID_Card holder) recognizing the ID_Card
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel [ICAO9303-1].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
Unpersonalized ID_Card	ID_Card material prepared to produce a personalized ID_Card containing an initialized and pre-personalized ID_Card’s chip.
User Data	All data (being not authentication data) stored in the context of the applications of the ID_Card as defined in [EACTR] and 1. being allowed to be *read out or written* solely by an authenticated terminal (in the sense of [EACTR2.02], sec. 3.2) respectively 2. being allowed to be *used* solely by an authenticated terminal (in the sense of [EACTR, sec. 3.2]) (the private Restricted Identification key; since the Restricted Identification according to [EACTR, sec. 4.5] represents just a functionality of the ID_Card, the key material needed for this functionality and stored in the TOE is considered here as ‘user data’) respectively 3. being allowed to be *used* solely by the authenticated ID_Card holder (the private signature key within the eSign application); from this point of view, the private signature key of the ID_Card holder is also considered as ‘user data’. 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
ATT	Authentication Terminal as defined in [EACTR], sec. 3.2
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
PP	Protection Profile
PUK	PIN Unblock Key
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 eSign application' is synonym.
SGT	Signature Terminal as defined in [EACTR], sec. 3.2
SSCD	Secure Signature Creation Device or Qualified Electronic Signature Creation Device means an electronic signature creation device which meets the requirements of [SSCDPP]
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]

Appendix Results of Cryptographic Assessment

491 The following cryptographic algorithms are used by the TOE to enforce its security policy:

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1.	Authenticity	Terminal Authentication, ECDSA-signature verification of card verifiable certificates using SHA-{1,224,256, 384, 512}	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 3 Appendix A.6	Verification of certificates (Terminal Authentication) FCS_COP.1.1/ SIG_VER VERIFY CERTIFICATE
2.	Authenticity	ECDSA-signature generation	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[ECCTR]	FCS_COP.1.1/ SSCD PSO COMPUTE DIGITAL SIGNATURE
3.	Authentication	PACEv2	[EACTR] (PACEv2),	Length of [Nonce|=128 bit	[EACTR] part 2 sec 3.2	FIA_UID.1/PACE FIA_UAU.1/PACE FIA_UAU.5 GENERAL AUTHENTICATE
4.	Authentication	Chip Authentication v.2 based on ephemeral-static ECDH in combination with AES	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 2 sec. 3.3 and part 3 annex A.4	FCS_CKM.1.1/DH_CA GENERAL AUTHENTICATE
5.	Authentication	Terminal Authentication v.2 based on ECDSA using SHA-{1,224,256, 384, 512}	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 2 sec. 3.4 and 3 annex A.6	FCS_COP.1.1/ SIG_VER EXTERNAL AUTHENTICATE
6.	Key Agreement	ECDH using SHA-{1, 256} For PACE and Chip Authentication	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 3 annex A.4	FCS_CKM.1.1/ DH_PACE FCS_CKM.1.1/ DH_CA
7.	Confidentiality	Secure Messaging, AES in CBC mode	[FIPS197]	|k|=128, 192, 256	[EACTR], part 3 annex E	FCS_COP.1.1/AES
8.	Integrity	Secure Messaging,	[FIPS197] (AES), [SP800-38B]	|k|=128, 192, 256	[EACTR], part 3 annex	FCS_COP.1.1/CMAC

		AES in CMAC mode	(CMAC)		E	
9.	Trusted Channel	Secure messaging in ENC_MAC mode is established during PACE	[EACTR] (PACE)	-	[EACTR]	FTP_ITC.1/PACE
10.	Trusted Channel	Secure messaging in ENC_MAC mode is established during Chip Authentication v2 after PACE	[EACTR]	-	[EACTR]	FTP_ITC.1/CA
11.	Cryptographic Primitive	Hybrid deterministic RNG DRG.4	[AIS31]	n.a.	[ECARDTR]	FCS_RND.1
12	Cryptographic Primitive	Hash for key derivation SHA-{1,224,256, 384, 512}	[FIPS 180]	n.a.	[EACTR]	FCS_COP.1/SHA
13	Key Generation	ECDSA key generation for Chip Authentication	[ECCTR]	224, 256, 320, 384 and 512	[EACTR]	FCS_CKM.1/CA_PICC

Table 15: Cryptographic algorithms used by TCOS Identity Card

492 All cryptographic algorithms listed in table 15 are implemented by the TOE because of the standards building the TOE application (e.g. [EACTR]). For that reason an explicit validity period is not given.

493 The strength of the cryptographic algorithms was not rated in the course of this evaluation. According to Technical Guideline [EACTR], the algorithms are suitable for securing integrity, authenticity and confidentiality of the stored data for Electronic Identity Cards.

References

[AIS31]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, 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, 30.12.2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243

[BACPP3.1]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0055-2009, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model; Version 3.1, Sept. 2012, CCMB-2012-09-001,
Part 2: Security functional components; Version 3.1, Sept. 2012, CCMB-2012-09-002,
Part 3: Security assurance components; Version 3.1, Sept. 2012, CCMB-2012-09-003

Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, September 2012, CCMB-2012-09-004

[EACPP2.3]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0026-2006, 2007-11-19

[EACPP3.1]

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

[EACTR][273]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents , Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20

[273] The Protection Profiles refer to older versions of this Technical Guideline. The references given in the PPs are adapted to the version 2.10.

[ECARDTR]

Technische Richtlinie TR-03116-2 für die eCard-Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, Stand 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-02

[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 180-4, Specifications for the Secure Hash Standard (SHS), 2012-03

[FIPS186]

Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), 2009-06

[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-0978-2016 for NXP Secure Smart Card Controller P60x144/080PVA, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016-02

[HWST] Security Target of the underlying hardware platform

NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE, Security Target Lite, Rev. 2.61 — 14 October 2015, BSI-DSZ-CC-0978

[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, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0061-2009, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-12-15

[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]

Security IC Platform Protection Profile, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007, 2007-06-15

[RFC5639]

M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[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

[TCOSADM]

Administrator's Guidance TCOS Identity Card Version 1.1 Release 2, T-Systems International GmbH, 2016-02