T · · Systems ·

Specification of the Security Target
TCOS Residence Permit Card Version 1.1
Release 1/SLE78CLX1440P

Version: 1.1.1/20130913

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS Residence Permit Card 1.1.1 (IFX)
Stand:	13.09.2013
Version:	1.1.1
Hardware Basis:	SLE78CLX1440P
Autor:	Ernst-G. Giessmann
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History[1]

Version	Date	Remark
1.1.1	2013-09-12	Final Version

1

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 Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P
TOE:	TCOS Residence Permit Card Version 1.1 Release 1/ SLE78CLX1440P
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, T-Systems International GmbH,TeleSec
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4 augmented.
General Status:	Final Document
Version Number:	1.1.1
Date:	2013-09-13
Certification ID:	BSI-DSZ-CC-0835
Keywords:	Residence Permit Card, eID, eSign, ePass, MRTD, PACE, EAC

3 The TOE is a ready for Personalization contact-less chip with an initialized filesystem according to [RPCARDPP] based like the TCOS Identity Cards on the Operation System TCOS developed at T-Systems International GmbH.

1.2 TOE Reference

4 The Security Target refers to the Product "TCOS Residence Permit Card Version 1.1 Release 1" (TOE) of T-Systems International GmbH for CC evaluation.

1.3 TOE Overview

5 The Target of Evaluation (TOE) addressed by the current Security Target is the electronic Residence Permit Card (RP_Card) representing a contactless smart card programmed according[2] to the Technical Guideline TR-03110 ([EACTR]) and being compliant to EU – Residence Permit Specification [EURPS]. For CC evaluation the following applications of corresponding product will be considered:

the Passport Application[3] (*ePassport*) containing the related user data[4] (incl. biometric data) as well as the data needed for authentication (incl. MRZ); this application the TOE is intended to be used by authorities, amongst other as a machine readable travel document (MRTD);

---

2 Note that the TOE fulfills the stronger requirements of the Version 2.10 of the Technical Guideline TR-03110, whereas the Protection Profile is based on the Version 2.03 ([EACTR2.03]) only.

3 as specified in [EACTR, Part 1, sec. 2.1.1], see also [ICAO9303-1]

4 according to [EACTR, Part 1]; see also Glossary below for definitions

the *eID*-Application[5] including the related user data[6] 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[7] containing data needed for generating qualified electronic signatures on behalf of the RP_Card holder as well as for user authentication; this application is intended to be used in the context of official and commercial services, where a qualified electronic signature of the RP_Card holder is required. The eSign application is optional: it means that it can optionally be activated on the RP_Card by a Certification Service Provider Issuer (or on his behalf) authorized by the RP_Card Issuer.

6 According to the Technical Guideline TR-03110 (cf. [EACTR, Part 1, 2.1.1]) the ePassport Application supports Passive Authentication, Password Authenticated Connection Establishment (PACE) with CAN and MRZ as part of the Standard and General Inspection Procedure, Terminal and Chip Authentication Version 2 as required in the General Inspection Procedure and also Basic Access Control (BAC), which is considered in this ST only as part of Extended Access Control (EAC) with Chip and Terminal Authentication Version 1.

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, Part 3, B.7]).

8 For the ePassport application, the RP_Card holder can control the access to his user data by conscious presenting his RP_Card to authorities[8] (CAN or MRZ authentication as specified in [EACTR, Part 1, 3.3]).

9 For the eID-application, the RP_Card holder can control the access to his user data by inputting his secret PIN (eID-PIN) or by conscious presenting his RP_Card to the authorities[9].

10 For the eSign application, the RP_Card holder can control the access to the digital signature functionality by conscious presenting his RP_Card to a Service Provider and using his secret Verification Authentication Data for this application: eSign-PIN[10].

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, since qualified electronic signatures will be generated by the eSign application. For security reasons this will not be enforced by the TOE.

---

5 as specified in [EACTR, Part 1, sec. 2.1.2]
6 according to [EACTR, Part 1]
7 as specified in [EACTR, Part 1, sec. 2.1.3]
8 CAN or MRZ user authentication, see [EACTR, Part 1, sec. 2.3]
9 eID-PIN or CAN user authentication, see [EACTR, Part 1, sec. 2.3 and Part 2, sec. 2.3]
10 CAN and eSign-PIN (VAD as specified in [SSCDPP, sec. 3.2.3.5]).), user authentication, see [EACTR, Part 2, sec. 2.3]

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 RP_Card issuer according to the Organizational Security Policies [RPCARDPP]. The TOE supports the standardized domain parameters mentioned in [RFC5639] (keylength 224, 256, 320, 384, 512 bit), and the NIST P-256 curve mentioned in [EACTR, Part 3, A.2.1.1] (keylength 256 bit) including the corresponding hash functions. PACE and hence the General Inspection Procedure require the use of AES, whereas due to compatibility reasons the Advanced Inspection Procedure with BAC may be used with 3DES (cf. [EACTR, PArt 3, A.2.3.1 and A.2.4.1]). This depends on the Initialization of the TOE. A more detailed description in given in the Administrator Guidance [TCOSADM]

13 The RP_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 may be relevant, and if so, the TOE will be identified in more detail as "TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P", otherwise the notion "TCOS Residence Permit Card Version 1.1 Release 1" will be used, indicating that this context applies to any realization regardless which hardware base is used. The SLE78CLX1440P chip is selected from the M7820 family. Note that the Chip Identifier Byte is not used in the TOE identification because it has no impact on the evaluation.

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 [RPCARDPP] 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[11] 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.

[11] activated or not yet activated on the RP_Card

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.

1.4.2 TOE security features for operational use

20 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 RP_Card under control of the RP_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 RP_Card,
- Self-protection of the TOE security functionality and the data stored inside.

1.4.3 Non-TOE hardware/software/firmware

21 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 ISO Standard ISO14443.

22 From the logical point of view, the TOE is able to distinguish between the following terminal types, which, hence, shall be available (see [EACTR], Part 1, 2.2):

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 RP_Card holder for generation of digital signatures.

23 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 inspection system or authentication terminal or signature terminal, the related Inspection or Authentication Procedures must be used.

24 The TOE supports the usage of EIS-GAP[12], BIS-PACE[13] (due to compliance with [PACEPassPP], see sec. PP Claims) and EIS-AIP-BAC[14] (due to compliance with

[12] EIS-GAP means General Authentication Procedure (GAP), i.e. PACE, terminal authentication (version 2), passive authentication with SO_C and chip authentication (version 2) with an Extended Inspection System (EIS)

[EURPS] and, hence, with [EACPP3.1], see sec. PP Claims) types of inspection systems as well as of authentication and signature terminals unconditionally using General Authentication Procedure (GAP). GAP offers the most functionality according to [EACTR] and the most extended protection of assets in the sense of the PP ([RPCARDPP]).

25 Using other types of inspection systems (e.g. BIS-BAC[15]) is out of the scope of the PP ([RPCARDPP]). Nevertheless the contained therein conformance claims require the TOE to fulfill the BAC PP [BACPP3.1]. These requirements are out of the scope of the current ST.

26 Since the inherent security properties of BAC protocol cannot withstand some attack scenarios with a high attack potential, the related threats are considered not to be allied with using EIS-AIP-BAC. Organizations being responsible for the operation of inspection systems (CVCAs and DVs) shall be aware of this context.

27 A [EACTR]-compliant terminal shall always start a communication session using PACE. If successfully, it shall then try to proceed with terminal and chip authentications as required by GAP in [EACTR]. The terminal will be authorized (depending on its certificate) as the EIS-GAP in the sense of [EACTR]. If the trial with PACE and GAP failed, the [EACTR]-compliant terminal may try to establish a communication session using other valid options as described above.

28 After the General Authentication Procedure has successfully been performed, the authenticated terminal can request for a sector-specific chip-identifier (Restricted Identification, see [EACTR, Part 2, 3.5, Part 3, 2.7]). Restricted Identification aims providing a temporary RP_Card identifier being specific for a terminal sector (pseudo-anonymization) and supporting revocation features ([EACTR, Part 2, 3.5]). The security status of RP_Card is not affected by Restricted Identification.

29 Concerning terminals for the eSign application, the parallels with the terminals as defined in [SSCDPP] are as follows: the Authentication Terminal in the context of [EACTR] (and of the current ST) is CGA in [SSCDPP]; the Signature Terminal in the context of [EACTR] represents a combination of SCA and HID in [SSCDPP].

30 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, Part 3, C.1].

31 The following table gives an overview which types of terminals shall be supported for which single application of the TOE, see [ICAO9303-1, 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).

---

13 BIS-PACE means Standard Inspection Procedure (SIP) with PACE, i.e. PACE and passive authentication with SO_D with a Basic Inspection System (BIS)

14 EIS-AIP-BAC means Advanced Inspection Procedure (AIP) with BAC, i.e. BAC, chip authentication, passive authentication with SO_D and terminal authentication (version 1) with an Extended Inspection System (EIS)

15 BIS-BAC means BAC and passive authentication with SO_D with an Basic Inspection System (BIS)

	Basic Inspection System using SIP with PACE (BIS-PACE, official terminal)	Extended Inspection System using AIP with BAC (EIS-AIP-BAC, official terminal)	Extended Inspection System using GAP (EIS-GAP, official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
ePassport	Operations: reading all Data Groups except DG3 and DG4 User Interaction: CAN or MRZ for PACE	Operations: reading only DG3 and DG4 and optional DG5 – DG13 User Interaction: MRZ for BAC	Operations: reading all Data Groups (incl. biometric ones) User Interaction: CAN or MRZ for PACE	No operations	No Operations
eID	No operations	No operations	Operations: reading all Data Groups User Interaction: CAN for PACE	Operations: writing a subset of Data Groups, reading all or a subset of Data Groups User Interaction: eID-PIN, eID-PUK or CAN for PACE	No Operations
eSign	No Operations	No Operations	No Operations	Operations: activating eSign application User Interaction: eID-PIN, eID-PUK or CAN for PACE In this context the terminal is equivalent the CGA in [SSCDPP] and implements the corresponding HID.	Operations: generating digital signatures[16] User Interaction: CAN for PACE, the eSign-PIN through the HID to access the signature function In this context the terminal is equivalent to the SCA in [SSCDPP] and may implement the corresponding HID

Table 1: RP_Card applications vs. terminal types

16 the TOE generates digital signature values, which support qualified electronic signatures

1.4.4 Life Cycle Phases Mapping

32 Following the protection profile PP0035 [PP0035, sec. 1.2.3] the life cycle phases of a TCOS RP_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

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

Life cycle phase 1 "Development"

34 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.

35 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.

36 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 RP_Card application and the guidance documentation is securely delivered to the RP_Card manufacturer.

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

Life cycle phase 2 "Manufacturing"

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

39 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.

40 The RP_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,

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

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

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

42 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.

43 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 RP_Card holder by the CSP. Note that the TOE has no contact interface. The eSign Application can be used through the contactless interface only.

44 For the TOE one pre-configured version (FSV01) of the file system applies. A detailed description of the sub-phases and the file system pre-configurations, including the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSADM].

45 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"

46 The personalization of the RP_Card includes

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

(ii) the enrolment of the RP_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 RP_Card,

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

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

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

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

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

50 *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”

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

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

53 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 RP_Card holder identified by the authorized terminal. Therefore no further Personalization procedure is required in Phase 7 (Operational Use).

54 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

55 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.

56 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.

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

1.4.5.2 TOE Logical Boundaries

58 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.

59 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).

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

61 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

62 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, September 2012,

Part 2: Security functional components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,

Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, Revision 4, Sept. 2012

63 as follows:

Part 2 extended,

Part 3 conformant.

64 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

65 This ST claims *strict* conformance to 'Common Criteria Protection Profile Electronic Residence Permit Card (RP_Card PP) [RPCARDPP]. This includes the following conformance claims.

66 This ST claims *strict* conformance to 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009' [EACPP3.1].

67 The conformance claim above covers the part of the security policy for the ePassport application of the TOE corresponding to the security policy defined in [EACPP3.1]. This conformance claim is a requirement of [EURPS, sec. 6.3] and, in such a way, enforces support of the EIS-AIP-BAC type of inspection system by the TOE.

68 This ST claims *strict* conformance to 'Common Criteria Protection Profile Electronic Passport using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-2010, version 0.92, 30th April 2010' [PACEPassPP].

69 The conformance claim above covers the part of the security policy for the ePassport application of the TOE corresponding to the security policy defined in [PACEPassPP]. This conformance claim enforces support of the BIS-PACE type of inspection system by the TOE.

70 This ST claims *strict* conformance to the CC Protection Profile Secure Signature Creation Device – Part 2: Device with key generation, Version 1.03, BSI-CC-PP-0059-2009 [SSCDPP].

71 The last conformance claim covers the part of the security policy for the eSign application of the TOE corresponding to the security policy defined in [SSCDPP] and, hence,

is applicable, if the *eSign* application is operational. In addition to [SSCDPP], the current ST specifies authentication and communication protocols (GAP) having to be used for the *eSign* application of the TOE. These protocols contribute to securing SVD-export, DTBS-import and VAD-import functionality.

72 The *eSign* application of the TOE is intended to support qualified electronic signatures. The main specific property distinguishing qualified electronic signatures from others is that they base on qualified certificates and are created by secure signature creation devices (SSCD) as the TOE represents. Since the current TOE (its part the eSign application) shall be used as SSCD due to the PP conformance claim above, the only specific difference remained is using qualified certificates for qualified signatures. Whether a certificate is qualified or not is a pure organizational issue from the point of view of the TOE which does not impact the TOE functionality. Therefore, the PP conformance claim above covers not only qualified signatures, but can also do this for advanced signatures under an appropriate interpretation of the organizational security policies P.CSP_QCert and P.QSign in [SSCDPP].

2.3 Package Claims

73 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.

74 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

75 The ST claims *strict* conformance to the following protection profiles as required there: ICAO-EAC PP (sec. 2.5 in [EACPP3.1]), PACE-Pass PP (sec. 2.5 in [PACEPassPP]) and SSCD Core PP (sec. 6.4 in [SSCDPP]). Due to this fact, the Protection Profile ([RPCARDPP]) distinguishs 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. In the Protection Profile ([RPCARDPP]) the rationale is given that TOE type, SPD statement, security objectives statement and security requirements statement for each PP are commensurate and the the SFR and SAR statements in the RP_Card Protection Profile ([RPCARDPP]) includes those from the other PPs.

3 Security Problem Definition

76 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

77 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 RP_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], Part 1, 2.2) respectively (ii) being allowed to be *used* solely by an authenticated terminal (in the sense of [EACTR, Part 1, 2.2]) (the private Restricted Identification key[17]) respectively (iii) being allowed to be *used* solely by the authenticated RP_Card holder (the private signature key within the eSign application). This asset covers 'User Data on the MRTD's chip' and 'Logical MRTD sensitive User Data' in [EACPP3.1], 'user data stored on the TOE' (object #1) in [PACEPassPP] as well as 'SCD' and 'DTBS/R' in [SSCDPP].	Confidentiality[18] Integrity Authenticity
2	user data transferred between the TOE and the service provider connected[19]	All data (being not authentication data) being transferred in the context of the applications of the RP_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 'User Data transferred between the TOE and the service provider connected (i.e. an authority represented by Basic Inspection System with PACE)' (object #2) in [PACEPassPP] and 'DTBS' in [SSCDPP].	Confidentiality[18] Integrity Authenticity

17 Since the Restricted Identification according to [EACTR, sec. 4.5] represents just a functionality of the RP_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.

18 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.

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

3	RP_Card tracing data	Technical information about the current and previous locations of the RP_Card gathered by inconspicuous (for the RP_Card holder) recognizing the TOE knowing *neither* CAN *nor* MRZ *nor* eID-PIN *nor* eID-PUK. TOE tracing data can be provided / gathered. This asset covers 'ePass tracing data' (object #3) in [PACEPassPP].	Unavailability[20]

Table 2: Primary assets

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

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

80 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. This asset covers the equivalent object #4 in [PACEPassPP].	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 covers the equivalent object #5 and 'Authenticity of the MRTD's chip' in [EACPP3.1].	Availability
6	TOE immanent secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality[21]. This asset covers the equivalent object #6 in [PACEPassPP].	Confidentiality Integrity
7	TOE immanent non-secret cryptographic keys	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Card/Chip and Document Security Objects SO_C and SO_D, respectively, containing digital signatures) used by the TOE in order to enforce its security functionality. This asset covers the respective object #7 in [PACEPassPP] and 'SVD' in [SSCDPP].	Integrity Authenticity
8	Secret RP_Card holder authentication data	Secret authentication information for the RP_Card holder being used for verification of the authentication attempts as authorized RP_Card holder: • eID-PIN and eID-PUK stored in the RP_Card as well as • eSign-PIN (and eSign-PUK, if any[22]) (i) stored in the RP_Card[23] and (ii) transferred to it[24].	Confidentiality Integrity

20 represents a prerequisite for anonymity of the RP_Card holder

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

Object No.	Asset	Definition	Property to be maintained by the current security policy
9	RP_Card communication establishment authorization data	Restricted-revealable[25] 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. This asset covers the respective object #8 in [PACEPassPP].	Confidentiality[25] Integrity

Table 3: Secondary assets

81 *Application Note 4*: RP_Card holder authentication and RP_Card communication establishment authorization data are representted 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[26] — 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.

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

Subjects and external entities

83 This ST considers the following subjects:

External Entity	Subject	Role	Definition
1	1	RP_Card holder	A person for whom the RP_Card issuer has personalized the RP_Card[27]. This entity is commensurate with 'MRTD Holder' in [EACPP3.1], 'ePass holder' (subject #1) in [PACEPassPP] and 'S.Signatory' in [SSCDPP]. Please note that an RP_Card holder can also be an attacker (s. below).
2	–	RP_Card presenter	A person presenting the RP_Card to a terminal[28] and claiming the identity of the RP_Card holder. This subject is commensurate with 'Traveler' in [EACPP3.1] and 'S.User' in [SSCDPP]. Please note that an RP_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 RP_Card holder. Service Provider uses the rightful terminals managed by a DV. This external entity is commensurate with the respective external entity #3 in [PACEPassPP].
4	2	Terminal	A terminal is any technical system communicating with the TOE through the

22 eSign-PIN and eSign-PUK are local secrets being valid only within the eSign application

23 is commensurate with RAD in [SSCDPP]

24 is commensurate with VAD in [SSCDPP]

25 The RP_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.

26 the input device of the terminal

27 i.e. this person is uniquely associated with a concrete electronic RP Card

28 in the sense of [EACTR]

External Entity	Subject	Role	Definition
			contactless interface. The role 'Terminal' is the default role for any terminal being recognized by the TOE as neither PCT nor BIS-PACE nor EIS-AIP-BAC nor EIS-GAP nor ATT nor SGT ('Terminal' is used by the RP_Card presenter). This entity is commensurate with 'Terminal' in [EACPP3.1] and the respective external entity #4 in [PACEPassPP].
5	3	PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the RP_Card and the related value presented to the terminal by the RP_Card presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the RP_Card using a shared password (CAN, eID-PIN, eID-PUK or MRZ). This entity is commensurate with the respective external entity #5 in [PACEPassPP]. See also [EACTR,Part 1, 2.3, Part 2, 2.4]
6	4	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an authority[29] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data of the RP_Card presenter with the stored biometrical data of the RP_Card holder). BIS-PACE is a PCT additionally supporting/applying the Passive Authentication protocol and is authorized[30] by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored in the ePassport application on the RP_Card. BIS-PACE in the context of [EACTR] (and of the RP Card PP) is similar, but not equivalent to the Basic Inspection System (BIS) as defined in [BACPP3.1]. This entity is commensurate with the respective external entity #6 in [PACEPassPP]. See also [EACPP3.1, chap. 3.2.1, G.1 and G.2].
7	5	Extended Inspection System using AIP with BAC (EIS-AIP-BAC)	A technical system being used by an inspecting authority[31] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-AIP-BAC is a Basic Inspection System (BIS) in the sense of [BACPP3.1] additionally supporting/applying Chip Authentication (incl. passive authentication and Terminal Authentication protocols in the context of AIP and is authorized[32] by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. EIS-AIP-BAC in the context of [EACTR] (and of the RP Card PP) is equivalent to the Extended Inspection System (EIS) as defined in [EACPP3.1]. See also [EACTR, Part 1, 2.2 and Part 3, C.4].
8	1	Extended Inspection System using GAP (EIS-GAP)	A technical system being used by an inspecting authority[33] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-GAP is a PCT additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of GAP and is authorized[34] by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. EIS-GAP in the context of [EACTR] (and of the RP Card PP) is similar, but not

29 concretely, by a control officer
30 by organizational measures
31 concretely, by a control officer
32 by issuing terminal certificates
33 concretely, by a control officer
34 by issuing terminal certificates

External Entity	Subject	Role	Definition
			equivalent to the Extended Inspection System (EIS) as defined in [EACPP3.1]. See also [EACTR, Part 1, 2.2 and Part 3, C.4].
9	2	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 RP_Card presenter as the RP_Card holder (using secret eID-PIN[35]), (ii) updating a subset of the data of the eID application and (iii) activating the eSign application. An Authentication Terminal is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols in the context of GAP and is authorized by the RP_Card Issuer through the Document Verifier of receiving branch (by issuing terminal certificates) to access a subset of the data stored on the RP_Card. See also [EACTR, Part 1, 2.2 and Part 3, C.4].
10	3	Signature Terminal (SGT)	A technical system 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 in the context of GAP and is authorized by the RP_Card Issuer through the Document Verifier of receiving branch (by issuing terminal certificates) to access a subset of the data stored on the RP_Card. See also [EACTR, Part 1, 2.2 and Part 3, C.4].
11	4	Document Verifier (DV)	An organization enforcing the policies of the CVCA and of a Service Provider (governmental or commercial organization) and managing 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, Part 3, 3.2.3]. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the RP_Card Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement[36] between the RP_Card Issuer und a foreign CVCA ensuring enforcing the RP_Card Issuer's privacy policy[37]). This entity is commensurate with 'Document Verifier' in [EACPP3.1] and with the respective external entity #7 in [PACEPassPP].
12	5	Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the RP_Card Issuer with respect to protection of user data stored in the RP_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-AIP-BAC, EIS-GAP, 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, Part 3, 3.2.3]. The Country Signing Certification Authority (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, Part 3, 2.1}. This entity is commensurate with 'Country Verifying Certification Authority' in [EACPP3.1] and with the respective external entity #8 in [PACEPassPP].
13	–	Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Card/Chip and Document Security Objects stored on the RP_Card for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR, Part 1, 1.1] and [ICAO9303-1]. This role is usually delegated to a Personalization Agent.

35 Secret eID-PUK can be used for unblocking the eID-PIN as well as the eSign-PIN and resetting the related retry counters.

36 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.

37 Existing of such an agreement may technically be reflected by means of issuing a $C_{CVCA\text{-}F}$ for the Public Key of the foreign CVCA signed by the domestic CVCA.

External Entity	Subject	Role	Definition
			This entity is commensurate with the respective external entity #9 in [PACEPassPP].
14	–	Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the RP_Card Issuer with respect to confirming correctness of user and TSF data stored in the RP_Card. The CSCA represents the country specific root of the PKI for the RP_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. [ICAO9303-1], 5.1.1. The Country Signing Certification Authority 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, Part 1, 1.2.1]. This entity is commensurate with the respective external entity #10 in [PACEPassPP].
15	–	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 can also issue qualified certificates. A CSP is the Certification Service Provider in the sense of [SSCDPP].
16	6	Personalization Agent	An organization acting on behalf of the RP_Card Issuer to personalize the RP_Card for the RP_Card holder by some or all of the following activities: (i) establishing the identity of the RP_Card holder for the biographic data in the RP_Card38, (ii) enrolling the biometric reference data of the RP_Card holder39, (iii) writing a subset of these data on the physical Residence Permit Card (optical personalization) and storing them in the RP_Card (electronic personalization) for the RP_Card holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card/Chip Security Object and the Document Security Object (ePassport) defined in [ICAO9303-1] (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 RP_Card Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role. This entity is commensurate with 'Personalization agent' in [EACPP3.1], the respective external entity #11 in [PACEPassPP] and 'Administrator' in [SSCDPP].
17	7	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the RP_Card Manufacturer completing the IC to the RP_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 RP_Card Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [EACPP3.1], and the respective external entity #12 in [PACEPassPP].
18	–	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognized by the TOE. This entity is commensurate with 'Attacker' in [EACPP3.1], the respective external entity #13 in [PACEPassPP] and 'Attacker' in [SSCDPP].

Table 4: Subjects and external entities[40]

38 relevant for the ePassport, the eID and the eSign applications

39 relevant for the ePassport application

40 This table defines external entities and subjects in the sense of [CC]. Subjects can be recognized by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC]).

84 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

85 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.

86 The following threats are adopted in the current ST (they initially derived from the ICAO-BAC PP [BACPP3.1], ICAO-EAC PP [EACPP3.1], and from the ID_Card [IDCARDPP]):

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

87 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.

88 *Application Note 5:* A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this threat is confined to only selected data groups (DG3, DG4) within the ePassport application.

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

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

90 An attacker is listening to the communication between the RP_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.

91 *Application Note 7*: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this threat is confined to only selected data groups (DG3, DG4) within the ePassport application.

T.Tracing **Tracing RP_Card**

92 An attacker tries to gather TOE tracing data (i.e. to trace the movement of the RP_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

---

From this point of view, the TOE itself does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognized by the TOE.

correct values of shared passwords (CAN, MRZ, eID-PIN, eID-PUK) in advance.
This item concerns the following application(s): ePassport, eID, eSign.

93 *Application Note 8*: A product using BAC (whatever the type of the inspection system is: BIS-BAC or EIS-AIP-BAC) cannot avert this threat in the context of the security policy defined in the PP and used in this ST. Hence, this threat is considered not to be allied with using EIS-AIP-BAC.

T.Counterfeit Counterfeiting RP_Card

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

T.Forgery Forgery of Data

95 An attacker fraudulently alters the User Data or/and TSF-data stored on the RP_Card or/and exchanged between the TOE and the service provider connected in order to outsmart either the authenticated terminal (BIS-PACE, EIS-AIP-BAC, EIS-GAP, ATT or SGT) by the means of changed RP_Card holder's related reference data (like biographic or biometric data or SCD/SVD) or the TOE by altering data being sent to the TOE (like DTBS/R). The attacker does it in such a way that the Service Provider (represented by the terminal connected) or the TOE 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.Abuse-Func Abuse of Functionality

96 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 also the misuse of the functions for the initialization and the personalization in the operational phase after delivery to the RP_Card holder.
This item concerns the following application(s): ePassport, eID, eSign.
This threat covers T.SigF_Misuse from [SSCDPP].

97 *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 RP_Card

98 An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the RP_Card or/and exchanged between the TOE and the service provider connected. 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.

99 *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

100 An attacker may perform physical probing of the RP_Card in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the RP_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 RP_Card.

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

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

102 *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 RP_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 RP_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

103 An attacker may cause a malfunction the RP_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 RP_Card outside the normal operating conditions, exploiting errors in the RP_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.

104 *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.

105 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also considers all threats of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application.

Threat identifier	Equivalent to / covered by item in the ([RPCARDPP])	Comments
T.Read_Sensitive_Data	T.Skimming	The threat T.Read_Sensitive_Data is covered by T.Skimming, because sensitive biometric reference data (DG3, DG4) stored on the RP_Card are part of the asset *user data stored on the TOE*.
T.Counterfeit	T.Counterfeit	All these threats have the similar definitions and address the same assets. Therefore a distinction between these threats is not necessary.
T.Forgery	T.Forgery	
T.Abuse-Func	T.Abuse-Func	
T.Information_Leakage	T.Information_Leakage	
T.Phys-Tamper	T.Phys-Tamper	
T.Malfunction	T.Malfunction	

106 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also considers all threats of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application.

Threat identifier	Equivalent to / covered by item in the ([RPCARDPP])	Comments
T.Skimming	T.Skimming	All these threats have the similar definitions and address the same assets. Therefore a distinction between these threats is not necessary.
T.Eavesdropping	T.Eavesdropping	
T.Tracing	T.Tracing	
T.Forgery	T.Forgery	
T.Abuse-Func	T.Abuse-Func	
T.Information_Leakage	T.Information_Leakage	
T.Phys-Tamper	T.Phys-Tamper	

107 Due to identical definitions and the same names they are not repeated here.

108 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also considers all threats of the SSCD PP [SSCDPP]. If the *eSign* application is operational then all these items are applicable. Formally, they only concern the *eSign* application. For the sake of completeness the threats are listed below. More details can be found in the SSCD PP [SSCDPP].

Threat identifier	Equivalent to / covered by item in the ([RPCARDPP])	Comments
T.SCD_Divulg	–	–
T.SCD_Derive	–	–
T.Hack_Phys	T.Phys-Tamper	–
T.SVD_Forgery	T.Forgery T.Eavesdropping	T.Forgery covers SVD stored; T.Eavesdropping covers SVD being sent to the CGA
T.SigF_Misuse	T.Abuse-Func	T.Abuse-Func covers T.SigF_Misuse
T.DTBS_Forgery	T.Skimming	T.Skimming covers a rightful SCA

Threat identifier	Equivalent to / covered by item in the ([RPCARDPP])	Comments
	T.Forgery	T.Forgery covers DTBS/R being sent to the TOE.
T.Sig_Forgery	–	–

109 *Application note 13*: If in the table above no comments are given, the threats from the SSCD PP [SSCDPP] are adopted exactly as decribed in this ST. For covered items we use in the following explicitly only the items of the RP_Card PP.

3.3 Organizational Security Policies

110 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 RP_Card

1. The RP_Card issuer issues RP_Cards and approves terminals complying with all applicable laws and regulations.
2. The RP_Card issuer guarantees the correctness of the user data (amongst other of those, concerning the RP_Card holder) and of the TSF-data permanently stored in the TOE[41].
3. The RP_Card issuer uses only such TOE's technical components (IC) which enable traceability of the RP_Cards in their manufacturing and issuing life phases, i.e. *before* they are in the operational phase.
4. If the RP_Card issuer authorizes a Personalization Agent to personalize the RP_Card for the RP_Card holder, the RP_Card issuer has to ensure that the Personalization Agent acts in accordance with the RP_Card issuer's policy.

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

P.Card_PKI PKI for Chip and Passive Authentication[42] (issuing branch)

112 *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 RP_Card issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the RP_Card. For this aim he runs a Country Signing Certification Authority (CSCA). The RP_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).

41 cf. Table 2 and Table 3 above

42 Passive authentication is considered to be part of the Chip Authentication protocol.

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 RP_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 RP_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/Chip Security Objects of the RP_Cards and (v) manage the Chip Authentication Key Pairs {SK_{PICC}, PK_{PICC}} used for the chip authentication as defined in the technical specification [EACTR, Part 1, 3.4, Part 2, 3.3].

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

P.Terminal_PKI PKI for Terminal Authentication (receiving branch)

113 *Application Note 15*: 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 RP_Card issuer shall establish a public key infrastructure for the card verifiable certificates used for terminal authentication. For this aim, the RP_Card issuer shall run a domestic Country Verifying Certification Authority (domestic CVCA) and may use already existing foreign CVCAs[43]. The RP_Card issuer shall make the CVCA Link Certificate available to the CSCA (who shall finally distribute it to its RP_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 Private Key secret and issue a self-signed CVCA Certificate (C_{CVCA}) having to be made available to the RP_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[44].
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)[45].

---

43 In this case there shall be an appropriate agreement between the RP_Card Issuer und a foreign CVCA ensuring enforcing the RP_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.

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

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

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, Part 1, 3.5 and Part 2, 3.4] and (v) install C_T, C_{DV} and C_{CVCA} in the rightful terminals operated by him.

114 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/Chip and Document Security Objects having to be stored on the RP_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)[46].
3. CSPs shall ensure that they issue their certificates exclusively for the rightful data (public signature key of the RP_Card holder)[47].

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

P.Terminal Abilities and trustworthiness of rightful terminals

1. Rightful terminals (BIS-PACE, EIS-AIP-BAC, EIS-GAP, authentication terminal and signature terminal, cf. the table on p. 10) shall be used by Service Providers and by RP_Card holders as defined in [EACTR, Part 2, 2.2].
2. They shall implement either the terminal parts of the PACE protocol [EACTR, Part 2, 3..2] (for BIS-PACE, EIS-GAP) or the terminal parts of the BAC protocol [EACTR, Part 1, Annex A] (for EIS-AIP-BAC), of the Terminal Authentication protocol [EACTR, Part 1, 3.5 and Part 2, 3.4], of the Passive Authentication with SO_C [EACTR, Part 1, 1.1], of the Chip Authentication protocol [EACTR, Part 1, 3.4 and Part 2, 3.3] and of the Passive Authentication with SO_D [EACTR, Part 1, 1.1] and use them – dependent on the type of terminal – in the order as required by [EACTR, Part 1, 1.2.4 and Part 2, 2.4]. A rightful terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).
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 RP_Card) in order to enable and to perform the terminal authentication as defined in [EACTR, Part 1, 3.5 and Part 2, 3.4].
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 with SO_C determination of the authenticity of PK_{PICC}, [EACTR, Part 1, 3.4 and Part 2, 3.3], and SO_D (determination of the authenticity of the data groups stored in the ePassport, [EACTR, Part 1, 1.1].

---

46 This rule is relevant for T.Skimming

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

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[48].
6. A rightful terminal and its environment shall ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PINs/PUKs, CAN and MRZ, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

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

115 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all OSPs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application.

OSP identifier from the PP	Equivalent to / covered by OSP in this ST	Comments
P.BAC-PP	see paragraph 25 (p. 9) and the Application Note 8 of the RP_Card PP ([RPCARDPP])	Fulfillment of the Basic Access Control Protection Profile is a matter of a different evolution, which is independent from the current ST. Because the TOE is already evaluated and certified in accordance with [BACPP3.1] (see [BACCR]) and BAC is outside the scope of the current ST this OSP will not be considered in the following.
P.Sensitive_Data	P.Terminal_PKI T.Eavesdropping	P.Terminal_PKI covers 'The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate.' T.Eavesdropping covers 'The MRTD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.'
P.Manufact	P.Pre-Operational	Because P.Manufact is covered by P.Pre-Operational, only the latter is considered in the following.
P.Personalization	P.Pre-Operational	Because P.Personalization is covered by P.Pre-Operational, only the latter is considered in the following.

Table 5: OSPs taken over from [EACPP3.1]

116 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all OSPs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. Due to identical definition and same name it is not neccessary to consider them separately and therefore they are not repeated here.

117 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all OSPs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. Formally, they only concern the *eSign* application. For the sake of completeness the OSPs are listed below. More details can be found in the SSCD PP [SSCDPP].

48 This rule is relevant for T.Skimming

OSP identifier from the PP	Equivalent to / covered by OSP in this ST	Comments
P.CSP_QCert	P.Trustworthy_PKI (partially)	P.Trustworthy_PKI covers rightful SVDs within related certificates. Additionally, CSP has to use a trustworthy CGA, to put correct names of the signatories into its certificates and to ensure that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information. Despite of that P.CSP_QCert is partially covered by P.Trustworthy_PKI, it will be considered in the following.
P.QSign		The TOE complies with these OSPs. For the coverage refer to [SSCDPP].
P.Sigy_SSCD		
P.Sig_Non-Repud		

Table 6: Table 7: OSPs taken over from [SSCDPP]

3.4 Assumptions

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

119 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST takes over all assumptions of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application.

Assumption identifier	covered by in this ST	Comments (see also [EACPP3.1] for better comparability)
A.MRTD_Manufact	ALC_DVS.2	see Application Note *16* below
A.MRTD_Delivery	ALC_DEL.1	
A.Pers_Agent	P.Pre-Operational P.Card_PKI	P.Pre-Operational covers ensuring the correctness of the logical MRTD with respect to the MRTD holder P.Card_PKI covers ensuring the correctness of keys and certificates stored on the MRTD's chip and signing the Document Security Object (SOD).
A.Insp_Sys	P.Terminal_PKI P.Terminal	P.Terminal_PKI covers availability of keys and certificates stored in the inspection system P.Terminal covers supporting necessary authentication protocols according to [EACTR].
A.Signature_PKI	P.Card_PKI	Because A.Signature_PKI is fulfilled due to compliance to P.Card_PKI, only the latter is considered in the following.
A.Auth_PKI	P.Terminal_PKI	Because A.Auth_PKI is fulfilled due to compliance to P.Terminal_PKI, only the latter is considered in the following.

Table 8: Assumptions taken over from [EACPP3.1]

120 *Application note 16:* Assumptions A.MRTD_Manufact and A.MRTD_Delivery from [EACPP3.1] address manufacturing, testing and delivery aspects. Fulfillment of such

assumptions is a necessary condition for a 'pass' judgement by applying the chosen assurance components ALC_DVS.2 and ALC_DEL.1, respectively. It means that if the respective assurance components ALC_DVS.2 and ALC_DEL.1 have positively been judged, the fulfilment of these assumptions is 'automatically' ensured: the manufacturer is required and responsible for applying all the related procedures with respect to the TOE. Therefore, the assumptions A.MRTD_Manufact and A.MRTD_Delivery are implicitly included by the RP_CARD PP ([RPCARDPP]) by choosing the assurance components ALC_DVS.2 and ALC_DEL.1. The remaining assumptions from [EACPP3.1] A.Pers_Agent, A.Insp_Sys, A.Signature_PKI and A.Auth_PKI are completely covered by the respective items (OSPs) defined in the RP_CARD PP. Hence we will explicitly use the items of this PP ([RPCARDPP]).

121 Since there are no assumptions in the PACE-Pass PP [PACEPassPP], there is nothing to be considered in this ST.

122 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST takes over all assumptions of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

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

Assumption identifier	Covered by in this ST	Comments (see also [SSCDPP] for better comparability)
A.CGA	-	This item concerns not only qualified, but also non-qualified certificates and will be considered in this ST.
A.SCA	P.Terminal (partially)	P.Terminal covers using trustworthy SCAs. Additionally, the SCA shall generate and send the DTBS/R to the TOE. Despite of that this assumption is partially covered, it will be considered in this ST.

Table 9: Assumptions taken over from [SSCDPP]

124 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.

125 The PP ([RPCARDPP]) does not include any additional assumptions. Hence there are explicitly only two assumptions A.CGA and A.SCA being exclusively applicable to the eSign application of the TOE.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.Data_Integrity Integrity of Data

128 The TOE must ensure integrity of the User Data and the TSF-data[49] 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[49] during their exchange between the TOE and the Service Provider connected (and represented by either BIS-PACE, EIS-AIP-BAC, EIS-GAP or ATT or SGT) after the PACE Authentication as well as the Terminal- and the Chip Authentication.

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

129 *Application Note 17*: A product using BIS-BAC cannot achieve this objective either for stored or being transmitted data in the context of the security policy defined in the ST. When using EIS-AIP-BAC, this objective is confined to only selected data groups (DG3, DG4) within the ePassport application.

OT.Data_Authenticity Authenticity of Data

130 The TOE must ensure authenticity of the User Data and the TSF-data[50] stored on it by enabling verification of their authenticity at the terminal-side[51].
The TOE must ensure authenticity of the User Data and the TSF-data[50] during their exchange between the TOE and the Service Provider connected (and represented be either BIS-PACE, EIS-AIP-BAC, EIS-GAP or ATT or SGT) after the PACE Authentication as well as 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 terminal) and by an active verification by the TOE itself (at receiving by the TOE)[52].

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

131 *Application Note 18:* A product using BIS-BAC cannot achieve this objective either for stored or being transmitted data in the context of the security policy defined in the ST. When using EIS-AIP-BAC, this objective is confined to only selected data groups (DG3, DG4) within the ePassport application.

---

49 where appropriate, see Table 3 above
50 where appropriate, see Table 3 above
51 verification of SO_C
52 Secure messaging after the chip authentication, see also [EACTR, sec. 4.4.2]

OT.Data_Confidentiality Confidentiality of Data

132 The TOE must ensure the confidentiality of the User Data and the TSF-data[53] by granting read access only to authorized rightful terminals (BIS-PACE, EIS-AIP-BAC, EIS-GAP, ATT, SGT) according to the effective terminal authorization level (CHAT)[54] presented by the terminal connected[55].
The TOE must ensure confidentiality of the User Data and the TSF-data[53] during their exchange between the TOE and the Service Provider connected (and represented be either BIS-PACE, EIS-AIP-BAC, EIS-GAP or ATT or SGT) after the PACE Authentication as well as the Terminal- and the Chip Authentication.

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

133 *Application Note 19*: A product using BIS-BAC cannot achieve this objective in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this objective is confined to only selected data groups (DG3, DG4)by granting read access only to authorized rightful terminal (EIS, ATT, SGT) according to the terminal authorization level (CHAT) presented by the terminal connected.

OT.Tracing Tracing RP_Card

134 The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the RP_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.

135 *Application Note 20:* A product using BAC (whatever the type of the inspection system is: BIS-BAC or EIS-AIP-BAC) cannot achieve this objective in the context of the security policy defined in the ST. Hence, this objective is considered not to be allied with using EIS-AIP-BAC.

OT.Chip_Auth_Proof Proof of RP_Card authenticity

136 The TOE must enable the terminal connected to verify the authenticity of the RP_Card as a whole device as issued by the RP_Card issuer (issuing PKI branch of the RP_Card issuer) by means of Passive (using SO_C) and Chip Authentication as defined in [EACTR, Part 1, 3.4 and Part 2, 3.3].

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

137 *Application Note 21:* The OT.Chip_Auth_Proof implies the RP_Card's chip to have a secret to prove its authenticity by knowledge, i.e. a Chip Authentication Private Key as

---

53 where appropriate, see Table 3 above

54 CHAT is not applicable to BIS (here: BIS-PACE). For BIS-PACE, table 1.2 in sec. 1.1 of [EACTR] (column PACE) shall be applied.

55 The authorization of the terminal connected (CHAT) is drawn from the terminal certificate chain used for the successful terminal authentication as defined in [EACTR, Part 1, 3.5 and Part 2, 3.4]4 and shall be a non-strict subset of the authorization defined in the Terminal Certificate (C_T), the Document Verifier Certificate (C_{DV}) and the C_{CVCA} in the certificate chain up to the Country Verifying Certification Authority of the RP_Card Issuer (receiving PKI branch of the RP_Card Issuer). The effective terminal authorization can additionally be restricted by the RP_Card holder by a respective input at the terminal.

TSF-data. The terminal shall have the reference data to verify the authentication attempt of RP_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/Chip Security Object (SO_C) signed by the Document Signer.

138 *Application Note 22*: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the chip (no Chip Authentication), a product using Basic Inspection System (whatever the used protocol is: BAC or PACE) cannot achieve this objective in the context of the security policy defined in the ST. Hence, this objective is considered not to be allied with using BIS-PACE.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

139 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

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

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

141 *Application Note 23:* 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

142 The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF-data and the RP_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

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

OT.Prot_Malfunction Protection against Malfunctions

144 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.

145 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

146 The TOE must provide means to store Initialization[56] 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 RP_Card.
This item concerns the following application(s): ePassport, eID, eSign.

OT.Personalization Personalization of RP_Card

147 The TOE must ensure that the user data (amongst other those concerning the RP_Card holder[57]) and the TSF-data permanently stored in the TOE can be written by authorized Personalization Agents only. The Card/Chip and Document Security Objects 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 taking responsibility for this *eSign* application, if the RP_Card holder had applied for this.
This item concerns the following application(s): ePassport, eID, eSign.

148 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all security objectives for the TOE of the ICAO-EAC PP [EACPP3.1] and the PACE-Pass PP [PACEPassPP]. Formally they only concern the *ePassport* application. . Due to identical definition and the similar naming[58] it is not neccessary to consider them separately and therefore they are not repeated here..

56 amongst other, IC Identification data

57 biographical and biometrical data as well as the SCD, if the eSign is operational

58 The three minor deviations in the names are only formally and therefore not relevant: OT.AC_Pers is covered by OT.Personalization, OT.Data_Int by OT.Data_Integrity and OT.Sens_Data_Conf by OT.Data_Confidentiality.

149 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all security objectives for the TOE of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

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

Objective identifier from[SSCDPP]	covered by in this ST	Comments
OT.Lifecycle_Security		Because these objectives from the SSCD PP ([SSCDPP]) are not covered by objectives of this ST they remain in force in the following.
OT.SCD/SVD_Gen		
OT.SCD_Unique		
OT.SCD_SVD_Corresp		
OT.SCD_Secrecy	OT.Data_Confidentiality (partially)	OT.Data_Confidentiality covers the confidentiality of the SCD at storage. Despite of that OT.SCD_Secrecy is partially covered by OT.Data_Confidentiality, it will be considered in the following for generation, signing and destruction of the SCD.
OT.Sig_Secure		Because these objectives from the SSCD PP ([SSCDPP]) are not covered by objectives of this ST they remain in force in the following.
OT.Sigy_SigF		
OT.DTBS_Integrity_TOE	OT.Data_Integrity	Because these objectives from the SSCD PP ([SSCDPP]) are covered by the listed objectives of this ST they will not be considered in the following.
OT.EMSEC_Design	OT.Prot_Inf_Leak	
OT.Tamper_ID	OT.Prot_Phys-Tamper OT.Prot_Malfunction	
OT.Tamper_Resistance	OT.Prot_Phys-Tamper	

Table 10: TOE objectives taken over from [SSCDPP]

4.2 Security Objectives for the Operational Environment

I. RP_Card issuer as the general responsible

151 The RP_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

152 The RP_Card issuer must issue RP_Cards and approve using the terminals complying with all applicable laws and regulations.

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

II. RP_Card issuer and CSCA: RP_Card's PKI (issuing) branch

153 The RP_Card issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Passive_Auth_Sign Authentication of RP_Card by Signature

154 The RP_Card issuer has to establish the necessary public key infrastructure as follows: The CSCA acting on behalf and according to the policy of the RP_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 RP_Card issuer, who makes them available to his own (domestic) CVCA as well as to the foreign CVCAs under agreement[59]. 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/Chip and Document Security Objects of genuine RP_Cards in a secure operational environment only. The digital signature in the Card/ Chip Security Object relates to all security information objects according to [EACTR, Part 3, Appendix A].
The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DS must sign exclusively correct Card/Chip Security Objects having to be stored on the RP_Cards.

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

This item also covers OE.CGA_SSCD and partially OE.SVD_Auth from Table 11 below for the eSign application.

OE.Chip_Auth_Key Chip Authentication Key

155 A Document Signer acting in accordance with the CSCA policy has to (i) generate the RP_Card's Chip Authentication Key Pairs {SK_{PICC}, PK_{PICC}} used for the chip authentication as defined in [EACTR, Part 1, 3.4 and Part 2, 3.3], (ii) sign and store the Chip Authentication Public Keys in the Chip Authentication Public Key Info (Appendix A of [EACTR]) and (iii) support Service Providers to verify the authenticity of the RP_Card's chips used for genuine RP_Cards by certification of the Chip Authentication Public Keys by means of the Card/ Chip Security Object. A Document Signer has also to manage Restricted Identification Key Pairs {SK_{ID}, PK_{ID}} [EACTR, Part 2, 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 11 below for the eSign application.

OE.Personalization Personalization of RP_Card

156 The RP_Card issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the RP_Card holder and create the biographical data for the RP_Card[60], (ii) enroll the biometric reference data of the RP_Card holder[61], (iii) write a subset of these data on the physical Identification Card (optical personalization) and store them in the RP_Card (electronic personalization) for the RP_Card holder as defi-

59 CVCAs represent the roots of the receiving branch, see below
60 relevant for the ePassport, the eID and the eSign applications
61 relevant for the ePassport application

ned in [EACTR], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Card/Chip Security and Document Objects 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 11 below for the eSign application.

III. RP_Card issuer and CVCA: Terminal's PKI (receiving) branch

157 The RP_Card issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the RP_Card issuer Card Issuer)[62] will implement the following security objectives of the TOE environment:

OE.Terminal_Authentication Authentication of rightful terminals

158 The RP_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 RP_Card issuer as well as each foreign CVCA acting under agreement with the RP_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 RP_Card issuer, (who makes it available to his own CSCA[63]) 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, 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 RP_Card. A DV has also to manage Sector's Static Key Pairs {$SK_{SectorNN}$, $PK_{SectorNN}$} [EACTR, Part 2, 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 1, 3.5 and Part 2 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)[64].

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

---

62 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.

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

64 This rule is relevant for T.Skimming

This item also partially covers OE.SVD_Auth from Table 11 below for the eSign application.

OE.Terminal Terminal operating

159 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 (BIS-PACE, EIS-AIP-BAC, EIS-GAP, authentication or signature terminals) as defined in [EACTR, PArt 1, 2.2].
2. Their terminals implement the terminal parts of the PACE protocol [EACTR, PArt 1,3.3 and PArt 2, 3.2] (for BIS-PACE, EIS-GAP), or the terminal parts of the BAC protocol [EACTR, Part 1, Appendix A] (for EIS-AIPBAC), of the Terminal Authentication protocol [EACTR, Part 1, 3.5 and Part 2, 2.4], of the Passive Authentication with SO_C [EACTR, Part 1, 1.1] (by verification of the signature of the Card/Chip Security Object) and of the Chip Authentication protocol [EACTR, Part 1, 3.4 and Part 2 , 3.3][65] and and of the Passive Authentication with SO_D [EACTR, Part 1, 1.1] and use them – dependent on the type of terminal – in the order[66] as required by [EACTR, Part 1, 2.2]. A rightful terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).
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 (CHAT) for access to the data stored on the RP_Card) in order to enable and to perform the terminal authentication as defined in [EACTR, Part 1, 3.5 and Part 2, 3.4].
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 with SO_C of the RP_Card (determination of authenticity of PK_{PICC}, [EACTR, Part 1, 3.3.1.2]) and SO_D (determination of authenticity of the data groups stored in the *ePassport* application [EACTR, Part 1, sec. 1.1]).
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[67].
6. Their terminals and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PINs/PUKs, CAN and MRZ, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

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

This item also partially covers OE.SVD_Auth, OE.HID_VAD, OE.DTBS_Intend from Table 11 below for the eSign application.

---

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

66 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 [RPCARDPP].

67 This rule is relevant for T.Skimming.

IV. RP_Card holder Obligations

OE.Card-Holder RP_Card holder Obligations

160 The RP_Card holder has to keep his or her verification values of eID-PIN and eID-PUK secret. The RP_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.

161 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all security objectives for the TOE's environment from the ICAO-EAC PP [EACPP3.1] and the PACE-Pass PP [PACEPassPP]. Formally they only concern the *ePassport* application. Due to the rationale given in the PP ([RPCARDPP]) all these objectives are implicitly covered by the objectives in the RP_Card PP ([RPCARDPP]). Hence they will not repeated in this ST.

162 Due to the strict conformance claims of the Protection Profile ([RPCARDPP]) this ST also includes all the security objectives for the TOE's environment of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational.

163 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 from [SSCDPP]	Equivalent to or covered by item in the ST	Comments
OE.SVD_Auth	OE.Passive_Auth_Sign (partially) OE.Terminal (partially)	OE.Passive_Auth_Sign and OE.Terminal cover ensuring the integrity of the SVD exported by the TOE to the CGA. Additionally, the CGA shall verify the correspondence between the SCD in the SSCD of the signatory and the SVD exported, cf. OE.SSCD_Prov_Service.
OE.CGA_QCert	OE.Personalisation (partially)	OE.Personalisation covers the correct identity of the Signatory (RP_Card holder). Additionally, CGA shall include the SVD matching the SCD stored in the TOE and the advanced signature of the CSP in its certificates. This item also ensures the property #3 (CSP duties) of P.Trustworthy_PKI
OE.SSCD_Prov_\ Service	OT.Chip_Auth_Proof	Because the objective OE.SSCD_Prov_Service is covered by OT.Chip_Auth_Proof it will not be considered in the following.
OE.HID_VAD	OE.Terminal	Because the objective OE.HID_VAD is covered by OE.Terminal it will not be considered in the following.
OE.DTBS_Intend	OE.Terminal (partially)	OE.Terminal covers enabling verification of the integrity of the DTBS/R by the TOE. Additionally, SCA shall (i) generate the DTBS/R of the data which the signatory intends to sign, (ii) send the DTBS/R to the TOE and (iii) attach the signature produced by the TOE to the data.
OE.DTBS_Protect	OT.Data_Integrity	The TOE's objective OT.Data_Integrity supports the objective OE.DTBS_Protect.
OE.Signatory	OE.Card-Holder (partially)	OE.Card-Holder covers keeping her Signatory VAD confidential.

Objective identifier from [SSCDPP]	Equivalent to or covered by item in the ST	Comments
		Additionally, Signatory has to check that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state.

Table 11: TOE's environment objectives taken over from [SSCDPP]

4.3 Security Objective Rationale

164 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.Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Personalization	OE.Passive_Auth_Sign	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Terminal	OE.Card-Holder	OE.Legislative_Compliance	OE.CGA_QCert ([SSCDPP])
T.Skimming			x	x	x										x	x	x		
T.Eavesdropping					x														
T.Tracing						x											x		
T.Counterfeit							x							x		x			
T.Forgery		x	x	x				x		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.Card_PKI													x	x					
P.Terminal_PKI															x				
P.Trustworthy_PKI													x		x				x

Table 12:Security Objective Rationale

165 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given in the RP_Card PP ([RPCARDPP]), ICAO-EAC PP [EACPP3.1], PACE-Pass PP [PACEPassPP] and SSCD PP [SSCDPP]. Hence it will not be repeated here.

166 For the Composite Evaluation the following Security Objectives for the Hardware Platform are relevant too. They are listed here for the sake of completeness only. The de-

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

167 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)

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

169 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.

5 Extended Components Definition

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

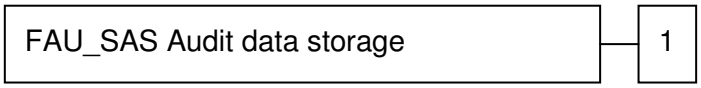
5.1 FAU_SAS Audit data storage

171 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.

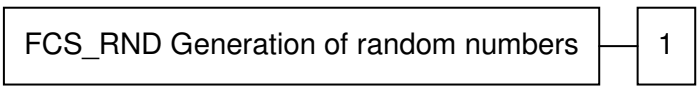
5.2 FCS_RND Generation of random numbers

172 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

173 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 Authentication Proof of Identity	1

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 FIA_APO Authentication Proof of Origin

174 The family “Authentication Proof of Origin (FIA_APO)” is specified as follows.

Family behavior

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

Component levelling:

FIA_APO.1 Authentication Proof of Origin.

Management: FIA_APO.1

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

Audit: FIA_APO.1

There are no actions defined to be auditable.

FIA_APO.1 Authentication Proof of Origin

Hierarchical to: No other components.

Dependencies: No dependencies.

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

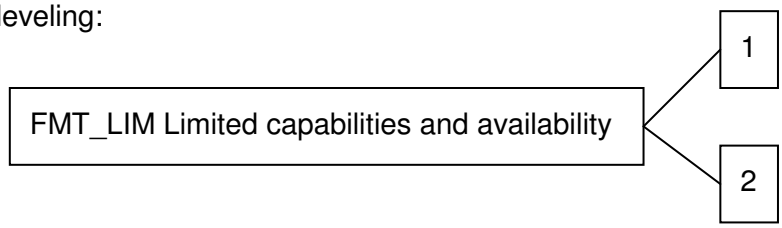
5.5 FMT_LIM Limited capabilities and availability

175 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.

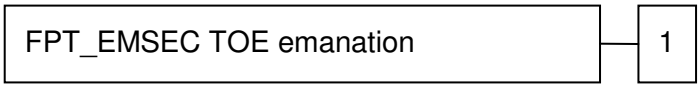
5.6 FPT_EMSEC TOE Emanation

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

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

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

Dependencies: No other components.

6 Security Requirements

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

177 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.

178 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~~.

179 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*.

180 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*.

181 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.

182 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

183 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 RP_CARD PP ([RPCARDPP]) 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 (BIS-PACE, EIS-GAP, ATT, SGT) – FIA_UAU.1/ICAO-EAC: Terminal Authentication (EIS-AIP-BAC) – {FDP_ACC.1/Signature-creation_SFP_SSCD, FDP_ACF.1/Signature-creation_SFP_SSCD}
Secure data exchange between the RP_Card and the Service Provider connected	– FTP_ITC.1/CA: trusted channel for EIS-AIP-BAC, EIS-GAP, ATT, SGT – FTP_ITC.1/PACE: trusted channel for BIS-PACE Supported by: a) for GAP: – FCS_COP.1/AES: encryption/decryption – FCS_COP.1/CMAC: MAC generation/verification – FIA_API.1/CA: Chip Identification/Authentication (version 2) – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (BIS-PACE, EIS-GAP, ATT, SGT) b) for AIP: – FCS_COP.1/SYM_ICAO-EAC: encryption/decryption – FCS_COP.1/MAC_ICAO-EAC: MAC generation/verification – FIA_API.1/ICAO-EAC: Chip Identification/Authentication (version 1) – FIA_UAU.1/ICAO-EAC: Terminal Authentication (EIS-AIP-BAC)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT equiv. BIS-PACE) – FIA_UID.1/Rightful_Terminal: Terminal Identification (EIS-GAP, ATT, SGT) – FIA_UID.1/ICAO-EAC: Terminal Identification (EIS-AIP-BAC) – FIA_UAU.1/PACE: PACE Authentication (PCT equiv. BIS-PACE) – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS-GAP, ATT, SGT) – FIA_API.1/CA: Chip Identification / Authentication for GAP (version 2) – FIA_UAU.1/ICAO-EAC: Terminal Authentication (EIS-AIP-BAC) – FIA_API.1/ICAO-EAC: Chip Identification/Authentication for AIP (version 1) – FIA_APO.1/PA_PACE-Pass: Passive Authentication using SO_D with previous PACE based on FIA_UAU.1/PACE (BIS-PACE) – 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 RP_Card holder as Signatory (eSign-PIN) – FIA_UIA.1/SSCD: Authentication of RP_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-AIP-BAC, EIS-GAP, ATT,

Security Functional Groups	Security Functional Requirements concerned
	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 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 13: Security functional groups vs. SFRs

184 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_{PCD}) as authentication reference data, (ii) the coded access control rights of the terminal (EIS-AIP-BAC, EIS-GAP, ATT, SGT), the Certificate Effective Date and the Certificate Expiration Date as security attributes.

Name	Data
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the RP_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/ Chip Security Object (SO_C) of the RP_Card and the Document Security Object (SO_D) of the ePassport application 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 RP_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). Note that the TOE provides several Chip Authentication Keys in different EFs (cf. [TCOSADM]).
Chip Authentication Private Key (SK_{PICC})	A 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]. SK_{PICC} is used by the TOE to authenticate itself as authentic RP_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 2 A.3, E.2.2, A.2.3.2.
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 terminal (EIS-AIP-BAC, EIS-GAP, ATT, SGT) as result of the Chip Authentication Protocol, see [EACTR], Part 2, A.4, and E.2.2, A.2.3.2.
Ephemeral keys	
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)	PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)
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 1, sec. 3 and Part 2, sec. 3]. 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 1, sec. 3 and Part 2, sec. 3]. For Restricted Identification please also refer to Paragraph 28 on p.5
Signature keys	
Signature Creation Key Pair (SCD/SVD)	Signature Creation Data (SCD) is represented by a private cryptographic key being used by the RP_Card holder (signatory) to create an electronic signature. This key represents user data. 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 14: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

185 **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][68] and specified cryptographic key sizes *112, 128, 192 and 256 bit*[69] that meet the following: [EACTR, Part 3, Appendix A.3[70].

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

186 *Application Note 24:* The TOE generates a shared secret value with the terminal during the PACE Protocol, see [EACTR, Part 1, 3.3 and Part 3, 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, E.2.2 and A.2.3] for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

187 *Application Note 25:* The TOE supports the following standardized elliptic curve domain parameters (cf. [EACTR]):

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]

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

---

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

189 **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][71] and specified cryptographic key sizes *112, 128, 192 and 256 bit*[72] that meet the following: [EACTR, Part 3, A.4][73].

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

190 *Application Note 26:* The TOE generates a shared secret value with the terminal during the CA Protocol, see [EACTR, Part 1, 3.4, Part 2, 3.3, and Part 3, A.4], which uses standardized domain parameters listed in Application Note 25 on p. 53. The shared secret value is used to derive the AES session keys for message encryption and message authentication (CA-K_{MAC}, CA-K_{Enc}) according to the [EACTR, Part 3, E.2.2 and A.2.3] for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

191 **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 **an ECDSA key** ~~cryptographic keys~~ in accordance with a specified cryptographic key generation algorithm *ECDSA key generation compliant to* [ECCTR][74] and specified cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order*[75] that meet the following: [EACTR][76].

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

---

71 [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]
72 [assignment: *cryptographic key sizes*]
73 [assignment: *list of standards*]
74 [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]
75 [assignment: *cryptographic key sizes*]
76 [assignment: *list of standards*]

192 *Application Note 27:* 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”.

193 *Application Note 28:* This SFR for Chip Authentication Key Pair Generation operation is added according to the recommendation of the Protection Profile [RPCARDPP, *Application note 68*].

194 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

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[77] that meets the following:

1. PACE: as specified in [EACTR, Part 1, 3.3, Part 2, 3.2 and Part 3, A.3];
2. CA: as specified in [EACTR, Part 2, 3.3 (version 2 for GAP) and Part 3, A.4][78].

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

195 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*[79] that meets the following: *none*[80].

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

77 [assignment: *cryptographic key distribution method*]
78 [assignment: *list of standards*]
79 [assignment: *cryptographic key destruction method*]
80 [assignment: *list of standards*]

196 *Application Note 29:* 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 destroys the CA Session Keys after detection of an error in a received command by verification of the MAC. The TOE clears 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.

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

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: not fulfilled, but justified:
A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.
FCS_CKM.4 Cryptographic key destruction: not fulfilled, but justified:
A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.

FCS_COP.1.1/ SHA	The TSF shall perform hashing[81] in accordance with a specified cryptographic algorithm *SHA-1, SHA-224 and SHA-256*[82] and cryptographic key sizes none[83] that meet the following: FIPS 180-2 [84].

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

198 *Application Note 30:* For hashing an ephemeral public key for DH (PACE[85] and CA[86]), the hash function SHA-1 will be used ([EACTR], Part 3, table A.3), but this is not relevant for the TOE. The TOE implements hash functions either SHA-1 or SHA-224 or SHA-256 for the Terminal Authentication Protocol (cf. [EACTR], Part 3, tables A.10 and A.11). Within the normative Appendix F of [EACTR, Part 3, E.2.3.1] 'Key Derivation' states that for deriving 128-bit AES keys the hash function SHA-1, whereas for deriving 192-bit and 256-bit AES keys SHA-256 shall be used.

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

---

81 [assignment: *list of cryptographic operations*]
82 [assignment: *cryptographic algorithm*]
83 [assignment: *cryptographic key sizes*]
84 [assignment: *list of standards*]
85 ID_{PICC} = H(ephem-PK_{PICC}-PACE) in [EACTR, sec. 4.4]
86 H(ephem-PK_{PCD}-TA) in [EACTR, sec. 4.3.1.2]

200 **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 personalization (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 ([RPCARDPP]) does not contain any dedicated requirement like FDP_ITC.2 for the import function.
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[87] in accordance with a specified cryptographic algorithm *ECDSA with plain signature format*[88] and cryptographic key sizes *192, 224, 256, 320, 384 and 512 bit length group order*[89] that meet the following: [EACTR][90].

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

201 *Application Note 31:* 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, A.6.3, A.6.4 and D.3 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 1, 3.4 and Part 2, 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).

202 *Application Note 32:* An ECDSA signature should use a hash function with a corresponding security level. The TOE supports SHA-224, SHA-256, SHA-384 and SHA-512 with the standardized domain parameters mentioned in [ECARDTR, section 1.3.2] and the NIST P-256 curve mentioned in [EACTR, Part 3, A.2.1.1].

203 **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

87 [assignment: *list of cryptographic operations*]
88 [assignment: *cryptographic algorithm*]
89 [assignment: *cryptographic key sizes*]
90 [assignment: *list of standards*]

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[91] in accordance with a specified cryptographic algorithm AES in CBC mode[92] and cryptographic key sizes *128, 192 and 256 bit*[93] that meet the following: FIPS 197 [FIPS197] and [EACTR, Part 3, Appendix E.2.2][94].

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

204 FCS_COP.1/SYM_ICAO-EAC Cryptographic operation – Encryption/Decryption DES

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/ SYM_ICAO-EAC	The TSF shall perform secure messaging – encryption and decryption[95] in accordance with a specified cryptographic algorithm *TDEA in CBC mode* [96] and cryptographic key sizes *112 bit*[97] that meet the following: FIPS 46-3 [FIPS46][98].

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

205 *Application Note 33*: These SFRs require the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the 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, E.2.1 and A.2.3.1] the (two-key) Triple-DES could be used in CBC mode for secure messaging. It is also a valid option in the ICAO-EAC PP [EACPP3.1] (see FCS_COP.1/SYM_ICAO-EAC). Due to the fact that the (two-key) Triple-DES is not recommended any more by the BSI, Triple-DES is applicable only to using EIS-AIP-BAC for reason of compliance with [EACPP3.1] and is also covered by [EACPP3.1]. For all

91 [assignment: *list of cryptographic operations*]
92 [assignment: *cryptographic algorithm*]
93 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256]
94 [assignment: *list of standards*]
95 [assignment: *list of cryptographic operations*]
96 [assignment: *cryptographic algorithm*]
97 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256]
98 [assignment: *list of standards*]

other terminal types being in the scope of the ST, Triple-DES in any mode is not applicable within this ST (cf. [RPCARDPP]).

206 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[99] in accordance with a specified cryptographic algorithm CMAC[100] and cryptographic key sizes *128, 192 or 256 bit*[101] that meet the following: [SP800-38B] and [EACTR, Part 3, E.2.2][102].

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

207 FCS_COP.1/MAC_ICAO-EAC Cryptographic operation – Retail MAC

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/ MAC_ICAO-EAC	The TSF shall perform secure messaging – message authentication code[103] in accordance with a specified cryptographic algorithm *Retail-MAC*[104] and cryptographic key sizes *112 bit*[105] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [ISO9797][106].

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

---

99 [assignment: *list of cryptographic operations*]
100 [assignment: *cryptographic algorithm*]
101 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit
102 [assignment: *list of standards*]
103 [assignment: *list of cryptographic operations*]
104 [assignment: *cryptographic algorithm*]
105 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit
106 [assignment: *list of standards*]

208 *Application Note 34*: These SFRs require the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the 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, Part 3, E.2.1 and A.2.3.1 the (two-key) Triple-DES could be used in Retail mode for secure messaging. It is also a valid option in the ICAO-EAC PP [EACPP3.1] (see FCS_COP.1/MAC_ICAO-EAC). Due to the fact that the Retail-MAC is not recommended any more by the BSI, this algorithm is applicable only to using EIS-AIP-BAC for reason of compliance with [EACPP3.1] and is also covered by [EACPP3.1]. For all other terminal types being in the scope of the ST this algorithm is not applicable within this ST (cf. [RPCARDPP]).

209 **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 *the quality requirements for a PTG.2 generator according to* [AIS31][107].

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

210 Application Note 35: This requirement is specified in [AIS31] in more details. The TOE implements a physical random number generator of the pre-defined class PRG.2 that provides the following security capabilities (PTG.2.1 to PTG.2.5) with a defined quality metric (PTG.2.6 and PTG.2.7):

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[108].

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

---

107 [assignment: *a defined quality metric*]

108 [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*]

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered *continuously*[109]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

The TSF provide *octets of bits*[110] that meet:

(PTG.2.6) Test procedure A[111] does not distinguish the internal random numbers from output sequences of an ideal RNG.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

211 *Application Note 36*: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols (PACE, CA and TA) as required by FIA_\ UAU.4. To avoid non-uniformity of the nonces generated during the PACE protocol additionally a cryptographic post-processing is applied. For a more detailed description of the security capabilities of the PTG.2 random number generator please refer to the hardware ST ([HWST]).

212 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application. For the functional class FCS, there are the following components: FCS_CKM.1/ICAO-EAC, FCS_CKM.4/ICAO-EAC, FCS_COP.1/SHA_\ ICAO-EAC, FCS_COP.1/SYM_ICAO-EAC, FCS_COP.1/MAC_ICAO-EAC, FCS_COP.1/ SIG_VER_ICAO-EAC, FCS_RND.1/ICAO-EAC.

213 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FCS, there are the following components: FCS_CKM.1/DH_PACE_PACE-Pass, FCS_CKM.2/DH_PACE-Pass, FCS_CKM.4/PACE-Pass, FCS_COP.1/AES_PACE-Pass, FCS_COP.1/MAC_PACE-Pass, FCS_RND.1/PACE-Pass.

214 The PP ([RPCARDPP]) demonstrates how the imported requirements are covered by its own requirements. Hence it is not repeated here. Additionally the use of Triple-DES and Retail-MAC is allowed (cf. Application Notes 33 and 34 on p. 57f)

215 This ST also includes all SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the *eSign* application is operational. Formally, they only concern the *eSign* application. For the functional class FCS there are the following components: FCS_CKM.1/SSCD, FCS_CKM.4/SSCD, FCS_COP.1/SSCD.

216 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

109 [selection: *externally, at regular intervals, continuously, applied upon specified internal events*]

110 [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]]

111 [assignment: *additional standard test suites*]

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][112] and specified cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order*[113] that meet the following: [EACTR][114].

217 *Application Note 37:* 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.

218 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.

FCS_COP.1.1/ SSCD	The TSF shall perform digital signature generation[115] in accordance with a specified cryptographic algorithm *ECDSA compliant to* [ECCTR][116] and cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order*[117] that meet the following: [ECCTR][118].

6.1.3 Class FIA Identification and Authentication

219 *Application Note 38:* The following Table 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 version 2 (for GAP)	FIA_UAU.1/Rightful_Terminal, FIA_UAU.5	as required by FCS_COP.1/SIG_VER

112 [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]
113 [assignment: *cryptographic key sizes*]
114 [assignment: *list of standards*]
115 [assignment: *list of cryptographic operations*]
116 [assignment: *cryptographic algorithm*]
117 [assignment: *cryptographic key sizes*]/[selection: 128, 192, 256] bit
118 [assignment: *list of standards*]

Chip Authentication Protocol version 2 (for GAP)	FIA_API.1/CA, FIA_UAU.5, FIA_UAU.6	as required by FCS_CKM.1/DH_CA
Terminal Authentication Protocol version 1 (for AIP)	FIA_UAU.1/ICAO-EAC, FIA_UAU.5/ICAO-EAC	inherited from [EACPP3.1]
Chip Authentication Protocol version 1 (for AIP)	FIA_API.1/ICAO-EAC, FIA_UAU.5/ICAO-EAC, FIA_UAU.6/ICAO-EAC	inherited from [EACPP3.1]
Passive Authentication using SOD	FIA_APO.1/PA_PACE-Pass	inherited from [PACEPassPP]
eSign-PIN	FIA_UAU.1/SSCD	inherited from [SSCDPP]

Table 15: Overview of authentication SFRs

220 **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 ≤ s_{ad} ≤ 6 *according to* [TCOSADM][119] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using eID-PIN as the shared password for PACE[120].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[121], the TSF shall suspend the reference value of eID-PIN according to [EACTR], sec. 3.3.2[122].

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

221 According to [EACTR], sec. 3.3.2, 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].

222 **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

119 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
120 [assignment: *list of authentication events*]
121 [selection: *met, surpassed*]
122 [assignment: *list of actions*]

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][123] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using suspended eID-PIN as the shared password for PACE[124].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[125], the TSF shall block the reference value of eID-PIN according to [EACTR, Part 2, 2.3.1][126].

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

223 *Application Note 39:* According to [EACTR, Part 2, 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 than $b_{ad} + s_{ad} \le 9$ overall tries of the eID-PIN are allowed.

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

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

FIA_AFL.1.1 The TSF shall detect when 1[127] unsuccessful authentication attempt~~s~~ occur**s** related to authentication attempts using CAN, MRZ, eID-PUK as shared passwords for PACE[128].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[129], the TSF shall *require the restart of the PACE protocol; and the TSF will increase the reaction time to the next authentication attempt*[130].

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

225 *Application Note 40*: The assignment operation reflects the fact that according the implementation the authentication procedure consumes a defined minimal amount of time.

123 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
124 [assignment: *list of authentication events*]
125 [selection: *met, surpassed*]
126 [assignment: *list of actions*]
127 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
128 [assignment: *list of authentication events*]
129 [selection: *met, surpassed*]
130 [assignment: *list of actions*]

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 does not represent a secret, because it may be revealed already to external entities (cf. footnote 25 on p. 19), 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.

226 *Application Note 41*: 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]).

227 **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, 3.3, Version 2 (for GAP)[131] to prove the identity of the TOE[132].

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

228 *Application Note 42:* 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 RP_Card by verifying the authentication token T_{PICC} calculated by the RP_Card using ephem-PK_{PCD}-TA and CA-K_{MAC}, (and, hence, finally making evident possessing the Chip Authentication Key (SK_{PICC})).
The Passive Authentication making evident authenticity of the PK_{PICC} by verifying the Card/Chip Security Object (SO_C) up to CSCA shall be triggered by the rightful terminal immediately after the successful Terminal Authentication before the Chip Authentication[133] 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.
Please note that the Chip Authentication Protocol according to [EACTR, Part 2, 3.3], version 1 (for AIP) is covered by [EACPP3.1] (see FIA_API.1 there).

131 [assignment: *authentication mechanism*]
132 [assignment: *authorized user or role*]
133 cf. [EACTR, sec. 3.4]

229 **FIA_APO.1/PA_PACE-Pass Authentication Proof of Origin**

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

FIA_API.1.1 The TSF shall provide the Passive Authentication according to [EACTR, Part 1, 1.1][134] to prove the origin of the ePassport[135].

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

230 *Application Note 43:* This SFR is taken over from the ePass_PACE PP ([EACPP3.1]), where it concerns the Passive Authentication of an electronic Passport (ePass). In the RP_Card the Passive Authentication is provided by the ePassport application of the TOE. Due to the identical naming of both applications the FIA_API.1 SFR can be adopted in this ST without changes.
The Passive Authentication making evident the authenticity/origin of data stored in the *ePassport* application by verifying the Document Security Object (SO_D) up to CSCA shall be triggered by the PCT immediately after the selection of *ePassport*. 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 origin of *ePassport* application. Independent of the result of Passive Authentication, secure messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

231 **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, 3.3][136]

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.

232 *Application Note 44:* 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 RP_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 RP_Card holder itself or an authorized other person or device.

134 [assignment: *authentication mechanism*]
135 [assignment: *authorized user or role*]
136 [assignment: *list of TSF-mediated actions*]

233 **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, sec. 4.2], 3. carrying out the Terminal Authentication Protocol according to [EACTR, Part 2, 3.4], Version 2 (for GAP)[137]. 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.

234 *Application Note 45:* The user identified after a successfully performed TA protocol is a rightful terminal, i.e. for GAP: either EIS-GAP or ATT or SGT.
Please note that the Terminal Authentication Protocol according to [EACTR,Part 2, 3.4], version 1 (for AIP) is covered by [EACPP3.1] (see FIA_UID.1 there). In this case, the user identified after a successfully performed TA protocol is also a rightful terminal, namely an EIS-AIP-BAC.

235 *Application Note 46:* 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 RP_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 like e.g. a 'privileged terminal', cf. [EACTR, Part 3, C.4, Table 21].

236 **FIA_UAU.1/PACE Timing of authentication**

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

FIA_UAU.1.1/ PACE	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE Protocol[138] according to [EACTR, Part 2 3.2][139]

137 [assignment: *list of TSF-mediated actions*]
138 RP_Card identifies themselves within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

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.

237 *Application Note 47:* 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 RP_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 RP_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.

238 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 2, 3.2], 3. carrying out the Terminal Authentication Protocol[140] according to [EACTR, Part 2, 3.4], Version 2 (for GAP) [141] 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.

239 *Application Note 48:* The user authenticated after a successfully performed TA protocol is a Service Provider represented by a rightful terminal, i.e. for GAP: either EIS-GAP 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, the terminal's compressed ephemeral public key **Comp**(ephem-PK_{PCD}-TA) from the accomplished TA. Please note that the Passive Authentication using SO_C is considered to be part of the CA

---

139 [assignment: *list of TSF-mediated actions*]
140 RP_Card identifies themselves within the TA protocol by using the identifier ID_{PICC} = H(ephem-PK_{PICC}-PACE).
141 [assignment: *list of TSF-mediated actions*]

protocol in the interpretation of the PP [RPCARDPP].

240 Please note that the Terminal Authentication Protocol according to [EACTR, Part 2, 3.4], version 1 (for AIP) is covered by [EACPP3.1] (see FIA_UAU.1 there). In this case, the user authenticated after a successfully performed TA protocol is also a Service Provider, concretely, an inspection system using EIS-AIP-BAC.

241 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 2, 3.2],
2. Terminal Authentication Protocol according to [EACTR, Part 2, 3.4], Version 2 (for GAP)[142].

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

242 *Application Note 49:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length length being (almost) uniformly distributed (the PP [RPCARDPP] supports the key derivation function based on AES; see [EACTR, Part 3, sec. A.3.3 and E.2.1). For the TA protocol, TOE randomly selects a nonce r_{PICC} of 64 bits length, see [EACTR, Part 3, B.3 and B.11.6].
Please note that the Terminal Authentication Protocol according to [EACTR, Part 2, 3.4], version 1 (for AIP) is covered by [EACPP3.1] (see FIA_UAU.4 there).

243 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 2, 3.2],
2. Terminal Authentication Protocol according to [EACTR, Part 2, 3.4], Version 2,
3. Chip Authentication Protocol according to [EACTR, Part 2, 3.3], Version 2,

and

4. Secure messaging in encrypt-then-authenticate mode according to [EACTR,Part 3 Appendix E][143]

to support user authentication.

---

142 [assignment: *identified authentication mechanism(s)*]
143 [assignment: *list of multiple authentication mechanisms*]

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[144] being successfully verifiable up to CVCA and (ii) the terminal uses the PICC identifier[145] 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[146].

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

244 *Application Note 50:* 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.
Please note that the Chip Authentication Protocol according to [EACTR, Part 2, sec. 3.3], version 1 (for AIP) is covered in this context by [EACPP3.1] (see FIA_UAU.5 there).

245 *Application Note 51:* 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.

246 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[147].

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

247 *Application Note 52:* 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 success-

144 PK_{PCD}
145 ID_{PICC} = H(ephem-PK_{PICC}-PACE)
146 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
147 [assignment: *list of conditions under which re-authentication is required*]

fully 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 the ephemeral key Comp(ephem-PK_{PCD}-TA).

248 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application and only the EIS-AIP-BAC terminal. For the functional class FIA, there are the following components: FIA_API.1/ICAO-EAC, FIA_UID.1/ICAO-EAC, FIA_UAU.1/ICAO-EAC, FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC and FIA_\ UAU.6/ICAO-EAC. According to the RP_Card PP the SFR FIA_UAU.6/ICAO-EAC is covered by other Security Requirements of this ST, therefore it will no be duplicated here.

249 FIA_API.1/ICAO-EAC 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 [EACTR1.11][148] to prove the identity of the TOE[149].

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

250 *Application Note 53:* In [EACTR, Part 2, 3.3] the Chip Authentication Mechanism as specified in [EACTR1.11] is called Chip Authentication Version 1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

251 FIA_UID.1/ICAO-EAC Timing of identification

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

FIA_UID.1.1/ICAO-EAC The TSF shall allow

1. establishing a communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. carrying out the Chip Authentication Protocol **according to [EACTR1.11]**[150].

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

148 [assignment: *authentication mechanism*]
149 [assignment: *authorized user or role*]
150 [assignment: *list of TSF-mediated actions*]

FIA_UID.1.2/ICAO-EAC	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.

252 *Application Note 54:* To distinguish the Chip and the Terminal Authentication Mechanisms as specified in [EACTR1.11] from the more general protocols with the same denotation defined in [EACTR, Part 2, 3.3] a corresponding refinement was made for the SFRs included from the ICAO-EAC PP [EACPP3.1].

253 FIA_UAU.1/ICAO-EAC Timing of authentication

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

FIA_UAU.1.1/ ICAO-EAC	The TSF shall allow 1. establishing a communication channel, 2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 3. to identify themselves by selection of the authentication key, 4. carrying out the Chip Authentication Protocol **according to [EACTR1.11]** [151] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/ ICAO-EAC	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.

254 FIA_UAU.4/ICAO-EAC 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/ ICAO-EAC	The TSF shall prevent reuse of authentication data related to[152] 1. Terminal Authentication Protocol Protocol **according to [EACTR1.11],** 2. Authentication Mechanism based on *AES*[153].

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

---

151 [assignment: *list of TSF-mediated actions*]
152 [assignment: *identified authentication mechanism(s)*]
153 [selection: *Triple-DES, AES or other approved algorithms*]

255 **FIA_UAU.5/ICAO-EAC Multiple authentication mechanisms**

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

FIA_UAU.5.1/ ICAO-EAC The TSF shall provide
1. Terminal Authentication Protocol **according to [EACTR1.11],**
2. Secure messaging in MAC-ENC mode
3. Symmetric Authentication Mechanism based on *AES*[154]

to support user authentication[155].

FIA_UAU.5.2/ ICAO-EAC The TSF shall authenticate any user's claimed identity according to the following rules:
1. The TOE accepts the authentication attempt as Personalization Agent by the *Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys*[156].
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism[157].

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

256 *Application Note 55:* The included from the ICAO-EAC PP requirements FIA_UID.1/ ICAO-EAC, FIA_UAU.1/ICAO-EAC, FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC and FIA_API.1/ICAO-EAC are restricted to the application of an EIS-AIP-BAC terminal, which is the only type of a General Inspection System (GIS in the sense of [EACPP3.1]) supporting Advanced Inspection Procedure version 1 with TDES considered in this ST. They are included in this ST only due to compatibility reasons and are not applicable to other authentication protocols.

257 This ST also includes all SFRs of the ePass_PACE PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FIA, there are the following components: FIA_AFL.1/PACE_PACE-Pass, FIA_APO.1/PA_PACE-Pass, FIA_\ UID.1/PACE_PACE-Pass, FIA_UAU.1/PACE_PACE-Pass, FIA_UAU.4/PACE-Pass, FIA_\ UAU.5/PACE-Pass, FIA_UAU.6/PACE-Pass.

---

154 [selection: *Triple-DES, AES or other approved algorithms*]
155 [assignment: *list of multiple authentication mechanisms*]
156 [selection: *the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys*]
157 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

258 The PP ([RPCARDPP]) demonstrates how the imported requirements are related, equivalent or covered by its corresponding own requirements. Hence it is not repeated here. Note that CA and TA protocols Version 1 are covered by these requirements.

259 This ST 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:

SFR identifier	Equivalent to / covered by item in the ST	Comments
FIA_UAU.1/SSCD	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.
FIA_UID.1/SSCD	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.
FIA_AFL.1/SSCD	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.

260 **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/ SSCD: The TSF shall allow
1. self test according to FPT_TST.1,
2. identification of the user by means of TSF required by FIA_UID.1/SSCD in [SSCDPP]
3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA[158],
4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA[159],
5. *none*[160]

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.

158 the authenticated terminal is ATT, cf. FIA_UAU.1/Rightful_Terminal
159 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
160 [assignment: *list of (additional) TSF-mediated actions*]

261 **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* [161]

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.

262 **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][162] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[163].

FIA_AFL.1.2/SSCD When the defined number of unsuccessful authentication attempts has been met[164], the TSF shall block RAD[165].

6.1.4 Class FDP User Data Protection

263 **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 [166] on terminals gaining write, read, modification and usage access to the User Data stored in the RP_Card [167].

---

161 [assignment: *list of additional TSF-mediated actions*]
162 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
163 [assignment: *list of authentication events*]
164 [selection: *met, surpassed*]
165 [assignment: *list of actions*]

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

264 **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 personalization 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[168] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. PACE Terminal (PCT equiv. BIS-PACE),
   c. Rightful Terminal (EIS-AIP-BAC, EIS-GAP, 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 RP_Card holder as Signatory (if the *eSign* is operational)[169].

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-GAP) is allowed to read User Data according to [EACTR, Part 3, C.4.1.1] 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

166 [assignment: *access control SFP*]
167 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
168 [assignment: *access control SFP*]
169 [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*]

(SCD/SVD Generation[170]) according to [EACTR, Part 3, C.4.1.2. 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, C.4.1.3] after a successful CA as required by FIA_API.1/CA and a successful authentication of the RP_Card holder as Signatory as required by FIA_UAU.1/SSCD[171].

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1. A successfully authenticated EIS-AIP-BAC is allowed to read User Data (only DG3 and DG4) according to [EACTR, Part 1, sec. 1.1 (ICAO/EAC version 1), Part 3, G.3 and C.4.1] after a successful TA as required by FIA_UAU.1/ ICAO-EAC (this rule is inherited from [PACEPassPP]).
2. A BIS-PACE (PCT) is allowed to read User Data (except DG3[172] and DG4[173]) according to [EACTR, Part 1, 1.1 and Part 3, G.2] after a successful PACE authentication as required by FIA_UAU.1/PACE_PACE-Pass (this rule is inherited from [PACEPassPP])[174].

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

1. Any terminal being not authenticated as a rightful terminal (i.e. as either BIS-PACE or EIS-AIP-BAC or EIS-GAP or ATT or SGT) is not allowed to read, to write, to modify, to use any User Data stored on the RP_Card.
2. Nobody is allowed to read 'TOE immanent secret cryptographic keys' stored on the RP_Card.
3. Nobody is allowed to read 'secret RP_Card holder authentication data' stored on the RP_Card.
4. Nobody is allowed to read the private Restricted Identification (SK_{ID}) key stored on the RP_Card.
5. Nobody is allowed to read the private signature key(s) within the eSign application (SCD; if the *eSign* application is operational[175].

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

---

[170] as required by FCS_CKM.1/SSCD

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

[172] biometric: finger

[173] biometric: iris

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

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

265 *Application Note 56*: 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, C.1.5]. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the RP_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]).

266 *Application note 57*: Please note that the Card/Chip Security Object (SO_C) does not belong to the user data, but to the TSF data. Read access to the Card/Chip Security Object is ruled by [EACTR, Part 3, A.1.2, Table 2] for EF.CardSecurity/EF.ChipSecurity, respectively. Also the Document Security Object (SO_D) stored in EF.SOD (see [ICAO9303-1], sec. A.10.4) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by the PCT as well as after accomplishing the BAC procedure, see [EACTR, Part 1, Annex A]. The Card/Chip Security Object can be read out by the PCT, see [EACTR, Part 3, A.1.2 and table 1 for EF.CardSecurity.

267 *Application Note 58*: 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, C.4.1.2] and acting on behalf of the CSP and upon an application by the RP_Card holder.

268 *Application note 59*: Please note that the control on the user data transmitted between the TOE and the rightful terminal is addressed by FTP_ITC.1/CA.

269 FDP_RIP.1 Subset residual information protection

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

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[176] the following objects:

1. the Chip Authentication Private Key (SK_{PICC}),
2. the secret RP_Card holder authentication data eID-PIN, eID-PUK, eSign-PIN (RAD, if *eSign* application is operational), (when their temporarily stored values are not to use any more),
3. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc}) (by closing related communication session),
4. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K[177]),
5. the private Restricted Identification key SK_{ID}, (when its tempo-

[176] [selection: *allocation of the resource to, de-allocation of the resource from*]
[177] according to [EACTR, Part 2, 3.2.1, #3.b

rarily stored value is not to use any more),
6. the private signature key of the RP_Card holder (SCD; if the *eSign* application is operational) (when its temporarily stored value is not to use any more),
7. *none*[178].

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

270 *Application Note 60*: The functional family FDP_RIP possesses such a general character, so that is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMSEC.

271 *Application Note 61*: Please note that FDP_RIP.1 also contributes to achievement of OT.Sigy_SigF (eSign-PIN) and OT.SCD_Secrecy (SCD) from [SSCDPP].

272 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application. For the functional class FDP, there are the following components: FDP_ACC.1/ICAO-EAC, FDP_ACF.1/ICAO-EAC, FDP_UCT.1/ICAO-EAC, FDP_UIT.1/ICAO-EAC.

273 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FDP, there are the following components: FDP_ACC.1/TRM_PACE-Pass, FDP_ACF.1/TRM_PACE-Pass, FDP_RIP.1/PACE-Pass,.

274 The PP ([RPCARDPP]) demonstrates how the imported requirements are related, equivalent or covered by its corresponding own requirements. Hence it is not repeated here.

275 This ST 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	
FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD	
FDP_ACC.1/SVD_Transfer_SFP_SSCD	
FDP_ACF.1/SVD_Transfer_SFP_SSCD	
FDP_ACC.1/Signature-creation_SFP_SSCD	
FDP_ACF.1/Signature-creation_SFP_SSCD	
FDP_RIP.1/SSCD	FDP_RIP.1 contributes to achievement of OT.Sigy_SigF (eSign-PIN) and OT.SCD_Secrecy (SCD)
FDP_SDI.2/Persistent_SSCD	
FDP_SDI.2/DTBS_SSCD	

276 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:

178 [assignment: *list of objects*]

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

277 *Application Note 62*: 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.

278 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[179] on

1. subjects: S.User
2. objects: SCD, SVD
3. operations: generation of SCD/SVD pair[180].

279 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

FDP_ACF.1.1/SCD/SVD_Generation_SFP_SSCD: The TSF shall enforce the SCD/SVD Generation SFP[181] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[182].

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:

179 [assignment: *access control SFP*]
180 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
181 [assignment: *access control SFP*]
182 [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*]

S.User with the security attribute “SCD/SVD Management” set to “authorized” is allowed to generate SCD/SVD pair[183].

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[184].
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[185].

280 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[186] on 1. subjects: S.User, 2. objects: SVD, 3. operations: export[187].

281 FDP_ACF.1/SVD_Transfer_SFP_SSCD Security attribute based access control

Hierarchical to: No other components.
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[188] to objects based on the following: 1. the S.User is associated with the security attribute Role, 2. the SVD[189].

183 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
184 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
185 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
186 [assignment: *access control SFP*]
187 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
188 [assignment: *access control SFP*]

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* [190] is allowed to export SVD[191].
FDP_ACF.1.3/ SVD_Transfer_SFP	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[192].
FDP_ACF.1.4/ SVD_Transfer_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[193].

282 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[194] on 1. subjects: S.User, 2. objects: DTBS/R, SCD, 3. operations: signature-creation[195].

283 FDP_ACF.1/Signature_Creation_SFP_SSCD Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/Signature_Creation_SFP_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[196] 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"[197].

---

189 [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*]
190 [selection: *R.Admin, R.Sigy*]
191 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
192 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
193 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
194 [assignment: *access control SFP*]
195 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
196 [assignment: *access control SFP*]

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[198].”
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[199].
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”[200].

284 **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[201] on all objects, based on the following attributes: integrity checked stored data[202].
FDP_SDI.2.2/Persistent_SSCD	Upon detection of a data integrity error, the TSF shall 1. prohibit the use of the altered data 2. inform the S.Sigy about integrity error[203].

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

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

---

197 [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*]
198 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
199 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
200 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
201 [assignment: *integrity errors*]
202 [assignment: *user data attributes*]
203 [assignment: *action to be taken*]

FDP_SDI.2.1/ DTBS_SSCD	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[204] on all objects, based on the following attributes: integrity checked stored DTBS[205].
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[206].

6.1.5 Class FTP Trusted Path/Channels

286 **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**[207] 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[208].

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

287 *Application note 63*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): 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.

288 **FTP_ITC.1/CA Inter-TSF trusted channel**

204 [assignment: *integrity errors*]
205 [assignment: *user data attributes*]
206 [assignment: *action to be taken*]
207 [selection: *the TSF, another trusted IT product*]
208 [assignment: *list of functions for which a trusted channel is required*]

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)**[209] to initiate communication via the trusted channel.
FTP_ITC.1.3/CA	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Service Provider represented by the rightful terminal after Chip Authentication[210].

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

289 *Application Note 64*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE), the TA protocol (FIA_UAU.1/Rightful_Terminal for GAP or FIA_UAU.1/ICAO-EAC for AIP) and the CA protocol (FIA_API.1/CA for GAP or FIA_API.1/ICAO-EAC for AIP). If the Chip Authentication was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc})[211]: this secure messaging enforces the required properties of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by (i) FCS_COP.1/AES and FCS_COP.1/CMAC for GAP or (ii) FCS_COP.1/SYM_ICAO-EAC and FCS_COP.1/MAC_ICAO-EAC for AIP being compliant with the ICAO EAC PP [EACPP3.1].

290 *Application Note 65*: Please note that the control on user data stored in the TOE is addressed by FDP_ACF.1/TRM.

291 *Application note 66*: The requirement FTP_ITC.1/CA also covers a secure transport of (i) SVD[212] from the TOE to CGA[213] as well as of (ii) VAD[214] from HID[215] and of (iii) DTBS[216] 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].

---

209 [selection: *the TSF, another trusted IT product*]
210 [assignment: *list of functions for which a trusted channel is required*]
211 otherwise, secure messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE
212 integrity is to secure
213 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]
214 confidentiality is to secure
215 the authenticated terminal is SGT
216 integrity is to secure

292 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. For the functional class FTP, there are no components there.

293 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FTP there is only one component FTP_ITC.1/PACE_PACE-Pass covered by FTP_ITC.1/PACE from the PP ([RPCARDPP]).

294 This ST also includes all SFRs of the SSCD PP [SSCDPP]. For the functional class FTP, there are no components there.

6.1.6 Class FAU Security Audit

295 FAU_SAS.1 Audit storage

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

FAU_SAS.1.1 The TSF shall provide the Manufacturer[217] with the capability to store the Initialization and Pre-Personalization Data [218] in the audit records.

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

296 *Application Note 67*: The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the RP_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 RP_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.

297 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. For the functional class FAU, there is only one component FAU_SAS.1/ICAO-EAC covered by FAU_SAS.1 from the PP ([RPCARDPP]).

298 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. For the functional class FAU, there is only one component FAU_SAS.1/PACE-Pass covered by FAU_\ SAS.1 from the PP ([RPCARDPP]).

299 This ST also includes all SFRs of the SSCD PP [SSCDPP]. For the functional class FAU there are no components there.

6.1.7 Class FMT Security Management

300 *Application Note 68*: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

---

217 [assignment: *authorized users*]
218 [assignment: *list of audit information*]

301 **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[219],
5. Activate and deactivate the eID-PIN[220].

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

302 **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 equiv. BIS-PACE),
7. Extended Inspection System using AIP with BAC(EIS-AIP-BAC),
8. Extended Inspection System using GAP (EIS-GAP),
9. Authentication Terminal (ATT),
10. Signature Terminal (SGT),
11. RP_Card holder[221].

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

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

303 *Application Note 69*: For the explanation on the role Manufacturer please refer to the Application Note 67; on the role Personalization Agent – to the Application Note 46. 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 RP_Card presenter). The). The

219 unblocking eSign-PIN is managed by FMT_SMF.1/SSCD
220 [assignment: *list of management functions to be provided by the TSF*]
221 [assignment: *the authorized identified roles*]

roles CVCA, DV, EIS, ATT[222] and SGT are recognized by analyzing the current Terminal Certificate C_T, cf. [EACTR, Part 3, C.4] (FIA_UID.1/Rightful_Terminal GAP or FIA_\ UAU.1/ICAO-EAC for AIP). The TOE recognizes the RP_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 .

304 *Application Note 70*: 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.

305 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[223].

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

306 FMT_LIM.2 Limited availability

Hierarchical to: No other components.
Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.

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

Deploying Test Features after TOE Delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. Embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[224].

---

222 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 authorization level, cf. [EACTR, sec. C.4.1.2]; an ATT with such a terminal authorization level is authorized by the related CSP to act as CGA on its behalf.

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

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

307 **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[225] the Initialization Data and Pre-personalization Data[226] to the Manufacturer[227].

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

308 **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[228] the Initialization Data[229] to the Personalization Agent[230].

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

309 *Application Note 71:* 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 46.

---

224 [assignment: *Limited capability and availability policy*]
225 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
226 [assignment: *list of TSF data*]
227 [assignment: *the authorized identified roles*]
228 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
229 [assignment: *list of TSF data*]
230 [assignment: *the authorized identified roles*]

310 **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[231] 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, A.6.2]
3. initial Current Date
4. *none*[232]

to *the Personalization Agent*[233].

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

311 *Application Note 72:* The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent in the issuing phase (cf. [EACTR, Part 3, 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, Part 3, 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]).

312 **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[234] the
1. Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the Country Verifying Certification Authority Certifi-

231 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
232 [assignment: *list of TSF data*]
233 [assignment: *the authorized identified roles*]
234 [selection: *change_default, query, modify, delete,* clear, [assignment: *other operations*]]

cate (C_{CVCA}) as required in [EACTR, Part 3, A.6.2]

3. *none*[235]

to Country Verifying Certification Authority[236].

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

313 *Application Note 73:* 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, Part 3, 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, Part 3, sec. 2.2.3 and 2.2.4]).

314 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[237] the Current Date[238] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Rightful Terminal (EIS, ATT or SGT) possessing an Accurate Terminal Certificate[239].

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

315 *Application Note 74*: The authorized roles are identified in their certificates (cf. [EACTR], Part 3, 2.2.4 and C.4]) and authorized by validation of the certificate chain up to CVCA (cf. 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, Part 3, A.6.2.3, B.11.1, C.1.3, C.1.5, D.2] for details).

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

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

235 [assignment: *list of TSF data*]
236 [assignment: *the authorized identified roles*]
237 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
238 [assignment: *list of TSF data*]
239 [assignment: *the authorized identified roles*]

FMT_MTD.1.1/PA_UPD	The TSF shall restrict the ability to write[240] the Card/Chip Security Object (SO_C) and the Document Security Object (SO_D)[241] to the Personalization Agent[242].

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

317 *Application Note 75*: By writing SO_C and SO_D into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. The latter consist of user data and TSF data, as well. Due to this fact and to the scope of the SFR FMT_MTD.1 (management of TSF-data), the entire set of the personalization data is formally not addressed above. Nevertheless, FMT_MTD.1/PA_UPD shall be understood in the following way: 'The TSF shall restrict the ability to write the personalization data to the Personalization Agent.' On the role 'Personalization Agent' please refer to the Application Note 46.

318 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*[243] the Chip Authentication Private Key (SK_{PICC})[244] to *Personalization Agent*[245].

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

319 *Application Note 76:* 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.

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

Hierarchical to: No other components.

---

240 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
241 [assignment: *list of TSF data*]
242 [assignment: *the authorized identified roles*]
243 [selection: *create, load*]/[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
244 [assignment: *list of TSF data*]
245 [assignment: *the authorized identified roles*]

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[246] the Chip Authentication Private Key (SK_{PICC})[247] to none[248].

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

321 **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[249] the suspended eID-PIN[250] to the RP_Card holder[251].

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

322 *Application Note 77:* 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, Part 2, 2.5.1] and is relevant for the status as required by FIA_AFL.1/eID-PIN_Suspending. The RP_Card holder is authenticated as required by FIA_UAU.1/ PACE using the eID-PIN as the shared password.

323 **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.

FMT_MTD.1.1/ eID-PIN_Unblock	The TSF shall restrict the ability to unblock and change[252] the blocked eID-PIN[253] to 1. the RP_Card holder, 2. the Authentication Terminal (ATT) with the Terminal Authorization Level for eID-PIN management[254].

246 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
247 [assignment: *list of TSF data*]
248 [assignment: *the authorized identified roles*]
249 [selection: *change_default, query, modify, delete,* clear, [assignment: *other operations*]]
250 [assignment: *list of TSF data*]
251 [assignment: *the authorized identified roles*]
252 [selection: *change_default, query, modify, delete,* clear, [assignment: *other operations*]]

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

324 *Application Note 78:* The unblocking procedure must be implemented according to [EACTR, Part 2, 2.5.2] and is relevant for the status as required by FIA_AFL.1/eID-PIN_\ Blocking. It can be triggered by either (i) the RP_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).

325 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[255] the eID-PIN[256] to the Authentication Terminal (ATT) with the Terminal Authorization Level for eID-PIN management[257].

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

326 *Application Note 79:* The activating/deactivating procedures must be implemented according to [EACTR, Part 2, 2.5.2]. 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).

327 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

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[258].

253 [assignment: *list of TSF data*]
254 [assignment: *the authorized identified roles*]
255 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
256 [assignment: *list of TSF data*]
257 [assignment: *the authorized identified roles*]
258 [assignment: *list of TSF data*]

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[259] of a successful authenticated Service Provider (represented by a rightful terminal).

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

328 *Application Note 80:* 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.

329 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application. For the functional class FMT, there are the following components: FMT_SMF.1/ICAO-EAC, FMT_SMR.1/ICAO-EAC, FMT_LIM.1/ICAO-EAC, FMT_LIM.2/ICAO-EAC, FMT_MTD.1/INI_ENA_ICAO-EAC, FMT_MTD.1/INI_DIS_ICAO-EAC, FMT_MTD.1/CVCA_INI_ICAO-EAC, FMT_MTD.1/CVCA_UPD_ICAO-EAC, FMT_\MTD.1/DATE_ICAO-EAC, FMT_MTD.1/KEY_WRITE_ICAO-EAC, FMT_MTD.1/CAPK_\ICAO-EAC, FMT_MTD.1/KEY_READ_ICAO-EAC, FMT_MTD.3/ICAO. Note that for BAC (EIS-AIP-BAC), the Document Basic Access Keys are derived from the value of the MRZ for the concrete instantiation of the TOE. Therefore, the Document Basic Access Keys are considered as a part of personalization data. FMT_MTD.1/KEY_READ covers the Document Basic Access Keys inherited from the ICAO-EAC PP. The concept of Personalization Agent Keys is covered by using an ATT proven a sufficient Terminal Authorization Level.

330 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FMT there are the following components: FMT_SMF.1/PACE-Pass, FMT_SMR.1/PACE-Pass, FMT_LIM.1/

259 This certificate-calculated Terminal Authorization Level can additionally be restricted by RP_Card holder at the terminal, s. [EACTR, sec. C.4.2]. It is based on Certificate Holder Authorization Template (CHAT); see [EACTR, C.1.5]. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the RP_Card holder's restricting input at the terminal. This final CHAT reflects the effective authorization level, see [EACTR, 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]).

PACE-Pass, FMT_LIM.2/PACE-Pass, FMT_MTD.1/INI_ENA_PACE-Pass, FMT_MTD.1/INI_DIS_PACE-Pass, FMT_MTD.1/PA_UPD_PACE-Pass.

331 The PP ([RPCARDPP]) demonstrates how the imported requirements are equivalent to or covered by its own requirements. Hence it is not repeated here. Additionally the use of Triple-DES and Retail-MAC is allowed (cf. Application Notes 33 and 34 on p. 57f)

332 This ST 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	R.Sigy is represented by the RP_Card holder, and R.Admin by the Personalization Agent, therefore it is covered by FMT_SMR.1
FMT_SMF.1/SSCD	–
FMT_MOF.1/SSCD	–
FMT_MSA.1/Admin_SSCD	–
FMT_MSA.1/Signatory_SSCD	–
FMT_MSA.2/SSCD	–
FMT_MSA.3/SSCD	–
FMT_MSA.4/SSCD	–
FMT_MTD.1/Admin_SSCD	–
FMT_MTD.1/Signatory_SSCD	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.

333 **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*[260].

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

334 **FMT_MOF.1/SSCD behaviour** **Management of security functions**

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
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[261] the functions signature-creation function[262] to R.Sigy[263].

335 **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,
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[264] to restrict the ability to modify[265] the security attributes SCD/SVD management[266] to R.Admin[267].

336 **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
FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD

FMT_MSA.1.1/ Signatory_SSCD: The TSF shall enforce the Signature-creation_SFP[268] to restrict the ability to modify[269] the security attributes SCD operational[270] to R.Sigy[271].

---

261 [selection: *determine the behavior of, disable, enable, modify the behavior of*]
262 [assignment: *list of functions*]
263 [assignment: *the authorized identified roles*]
264 [assignment: *access control SFP(s), information flow control SFP(s)*]
265 [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]
266 [assignment: *list of security attributes*]
267 [assignment: *the authorized identified roles*]
268 [assignment: *access control SFP(s), information flow control SFP(s)*]
269 [selection: *change_default, query, modify, delete,* [assignment: *other operations*]]

337 **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

FMT_MSA.2.1/ SSCD: The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[272].

338 Application Note 81: 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.

339 **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

FMT_MSA.3.1/ SSCD: The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature-creation SFP[273] to provide restrictive[274] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ SSCD: The TSF shall allow the R.Admin[275] to specify alternative initial values to override the default values when an object or information is created.

340 **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

270 [assignment: *list of security attributes*]
271 [assignment: *the authorized identified roles*]
272 [selection: *list of security attributes*]
273 [assignment: *access control SFP*, *information flow control SFP*]
274 [selection choose one of: *restrictive, permissive*, [assignment: *other property*]]
275 [assignment: *the authorized identified roles*]

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[276].

341 *Application Note 82:* Because the TOE does not support SCD/SVD generation by the Signatory alone, the rule (2) is not relevant here.

342 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
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[277] the RAD[278] to R.Admin[279].

343 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
FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCD

FMT_MTD.1.1/ Signatory_SSCD	The TSF shall restrict the ability to modify[280] the RAD[281] to R.Sigy[282].

276 [assignment: *rules for setting the values of security attributes*]
277 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
278 [assignment: *list of TSF data*]
279 [assignment: *the authorized identified roles*]
280 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
281 [assignment: *list of TSF data*]
282 [assignment: *the authorized identified roles*]

6.1.8 Class FPT Protection of the Security Functions

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

345 **FPT_EMSEC.1 TOE Emanation**

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

FPT_EMSEC.1.1 The TOE shall not emit *power variations, timing variations during command execution*[283] in excess of *non-useful information*[284] 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)[285]
3. *none*[286]

and

4. the private Restricted Identification key SK_{ID},
5. the private signature key of the RP_Card holder (SCD; if the *eSign* is operational)[287].
6. *none*[288]

FPT_EMSEC.1.2 The TSF shall ensure any users[289] are unable to use the following interface RP_Card’s contactless interface and circuit contacts[290] to gain access to

1. the Chip Authentication Private Key (SK_{PICC}),
2. the eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational),
3. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc}),
4. the ephemeral private key ephem-SK_{PICC}-PACE[291]
5. *none*[292]

283 [assignment: *types of emissions*]
284 [assignment: *specified limits*]
285 [assignment: *list of types of TSF data*]
286 [assignment: *list of types of (further) TSF data*]
287 [assignment: *list of types of user data*]
288 [assignment: *list of types of (further) user data*]
289 [assignment: *type of users*]
290 [assignment: *type of connection*]
291 [assignment: *list of types of TSF data*]

and

6. the private Restricted Identification key SK_{ID},
7. the private signature key of the RP_Card holder (SCD; if the *eSign* is operational)[293].
8. *none*[294].

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

346 *Application Note 83*: 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 RP_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.

347 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*[295].

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

348 FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation*[296] to demonstrate the correct operation of the TSF[297].

---

292 [assignment: *list of types of (further) TSF data*]
293 [assignment: *list of types of user data*]
294 [assignment: *list of types of (further) user data*]
295 [assignment: *list of types of failures in the TSF*]
296 [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*]]
297 [selection: [assignment: *parts of TSF*], *the TSF*]

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[298].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[299].

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

349 *Application Note 84*: The RP_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.

350 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[300] to the TSF[301] by responding automatically such that the SFRs are always enforced.

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

351 *Application Note 85*: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

352 This ST also includes all SFRs of the ICAO-EAC PP [EACPP3.1]. Formally, they only concern the *ePassport* application. For the functional class FPT, there are the following components: FPT_EMSEC.1/ICAO-EAC, FPT_FLS.1/ICAO-EAC, FPT_TST.1/ICAO-EAC, FPT_PHP.3/ICAO-EAC.

353 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. Formally, they only concern the *ePassport* application. For the functional class FPT there are the following components: FPT_EMSEC.1/PACE-Pass, FPT_FLS.1/PACE-Pass, FPT_TST.1/PACE-Pass, FPT_PHP.3/PACE-Pass.

---

298 [selection: [assignment: *parts of TSF*], *TSF data*]
299 [selection: [assignment: *parts of TSF*], *TSF*]
300 [assignment: *physical tampering scenarios*]
301 [assignment: *list of TSF devices/elements*]

354 The PP ([RPCARDPP]) demonstrates how the imported requirements are equivalent to or are covered by its own requirements. Hence it is not repeated here.

355 This ST 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
FPT_EMSEC.1/SSCD	This SFR is covered by FPT_EMSEC.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

356 **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

357 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

358 The following table provides an overview for security functional requirements coverage. It replicates the corresponding table 24 of the Protection Profile [RPCARDPP]. The missing columns are moved to the next table related to the SSCD PP [SSCDPP].

	OT.Identification	OT.Personalization	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
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						
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/SYM_ICAO-EAC			x	x	x		x				
FCS_COP.1/CMAC			x	x			x				
FCS_COP.1/MAC_ICAO-EAC			x	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_API.1/ICAO-EAC							x				
FIA_APO.1/PA_PACE-Pass			x	x							
FIA_UID.1/PACE			x	x	x						
FIA_UID.1/Rightful_Terminal		x	x	x	x						

	OT.Identification	OT.Personalization	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FIA_UID.1/ICAO-EAC			x	x	x						
FIA_UAU.1/PACE			x	x	x						
FIA_UAU.1/Rightful_Terminal		x	x	x	x						
FIA_UAU.1/ICAO-EAC			x	x	x						
FIA_UAU.4			x	x	x						
FIA_UAU.4/ICAO-EAC			x	x	x						
FIA_UAU.5			x	x	x						
FIA_UAU.5/ICAO-EAC			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									
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_EMSEC.1									x		
FPT_FLS.1									x		x
FPT_TST.1									x		x
FPT_PHP.3			x						x	x	

Table 16: Coverage of Security Objectives for the TOE by SFR

359 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 16 above. For convienence the table of mappings is given below. Note that according to Table 10 the objectives OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Prot_Phys-Tamper, OT.Prot_Malfunction and OT.Tamper_Resistance identified in the SSCD PP are replaced by the corresponding ST objectives OT.Data_Integrity, OT.Prot_Inf_Leak, OT.Tamper_ID and OT.Prot_Phys-Tamper.

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.Data_Integrity (OT.DTBS_Integrity_TOE)	OT.Prot_Inf_Leak (OT.EMSEC_Design)	OT.Tamper_ID (OT.Prot_Phys-Tamper and OT.Prot_Malfunction)	OT.Prot_Phys-Tamper (OT.Tamper_Resistance)
FCS_CKM.1/SSCD	x		x	x	x						
FCS_CKM.4	x				x						
FCS_COP.1/SSCD	x					x					
FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD	x	x									
FDP_ACC.1/SVD_Transfer_SFP_SSCD	x										
FDP_ACC.1/Signature-creation_SFP_SSCD	x						x				
FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD	x	x									
FDP_ACF.1/SVD_Transfer_SFP_SSCD	x										
FDP_ACF.1/Signature-creation_SFP_SSCD	x						x				
FDP_RIP.1					x		x				
FDP_SDI.2/Persistent_SSCD				x	x	x					
FDP_SDI.2/DTBS_SSCD							x	x			
FIA_AFL.1/SSCD							x				
FIA_UAU.1/SSCD		x					x				
FIA_UID.1/SSCD		x					x				
FMT_MOF.1/SSCD	x						x				
FMT_MSA.1/Admin_SSCD	x	x									
FMT_MSA.1/Signatory_SSCD	x						x				
FMT_MSA.2/SSCD	x	x					x				
FMT_MSA.3/SSCD	x	x					x				
FMT_MSA.4/SSCD	x	x					x				
FMT_MTD.1/Admin_SSCD	x						x				
FMT_MTD.1/Signatory_SSCD	x						x				

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.Data_Integrity (OT.DTBS_Integrity_TOE)	OT.Prot_Inf_Leak (OT.EMSEC_Design)	OT.Tamper_ID (OT.Prot_Phys-Tamper and OT.Prot_Malfunction)	OT.Prot_Phys-Tamper (OT.Tamper_Resistance)
FMT_SMR.1	x						x				
FMT_SMF.1/SSCD	x						x				
FPT_EMSEC.1					x				x		
FPT_FLS.1					x						
FPT_PHP.1/SSCD										x	
FPT_PHP.3					x						x
FPT_TST.1	x				x	x					

Table 17: Coverage of Security Objectives for the TOE by SFR

360 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the PP ([RPCARDPP]) and repeated below.

361 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.

362 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[302]. 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 achieve-

302 These Requirements 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.

ment 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.

363 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.
Unauthorized 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_APO.1/PA_PACE-Pass requires performing Passive Authentication using SOD for enabling the verification of the integrity of User Data stored on the TOE.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used. This also applies to FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC, FCS_CKM.4 and the Advanced Inspection Procedure for EIS-AIP-BAC terminals.
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 or FCS_COP.1/SYM_ICAO-EAC and FCS_COP.1/MAC_ICAO-EAC related to secure messaging for a EIS-AIP-BAC terminal. A prerequisite for establishing the 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 and for EIS-AIP-BAC terminals the corresponding FIA_API.1/ICAO-EAC, FIA_UAU.5/ICAO-EAC. 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 cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

364 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 or FCS_\ COP.1/SYM_ICAO-EAC and FCS_COP.1/MAC_ICAO-EAC related to secure messaging for a EIS-AIP-BAC terminal. A prerequisite for establishing the 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}). FIA_APO.1/PA_PACE-Pass requires performing Passive Authentication using SOD for enabling the verification of the authenticity of User Data stored on the TOE.
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. This also applies to FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC, FCS_CKM.4 and the Advanced Inspection Procedure for EIS-AIP-BAC terminals.
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.

365 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. This also applies to FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC, FCS_CKM.4 and the Advanced Inspection Procedure for EIS-AIP-BAC terminals.
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 or FCS_COP.1/SYM_ICAO-EAC and FCS_COP.1/MAC_ICAO-EAC related to secure messaging for a EIS-AIP-BAC terminal. A prerequisite for establishing the 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 (including the corresponding iterations for EIS-AIP-BAC terminals). 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.

366 The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the RP_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) – by 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) – by FTP_ITC.1/CA.

367 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.

368 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.

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

370 This objective is achieved

- by FPT_EMSEC.1 for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by FPT_FLS.1 and FPT_TST.1 for forcing a malfunction of the TOE, and
- by FPT_PHP.3 for a physical manipulation of the TOE.

371 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.

372 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.

373 The TOE Security Requirements sufficiency given in Chapter 11.1.2 of the SSCD PP shows that the objectives from that PP are supported by the SFRs from the TOE.

374 **OT.Lifecycle_Security** (Lifecycle security) is provided by the SFR for SCD/SVD generation FCS_CKM.1/SSCD, SCD usage FCS_COP.1/SSCD and SCD destruction FCS_CKM.4 ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation_\ SFP_SSCD and FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer_\ SFP_SSCD and FDP_ACF.1/SVD_Transfer_SFP_SSCD. The SCD usage is ensured by access control FDP_ACC.1/Signature-creation_SFP_SSCD, FDP_AFC.1/Signature-creation_SFP_SSCD which is based on the security attribute secure TSF management according to FMT_MOF.1/SSCD, FMT_MSA.1/Admin_SSCD, FMT_MSA.1/ Signatory_\ SSCD, FMT_MSA.2/SSCD, FMT_MSA.3/SSCD, FMT_MSA.4/SSCD, FMT_MTD.1/ Admin_SSCD, FMT_MTD.1/Signatory_SSCD, FMT_SMF.1/SSCD and FMT_SMR.1. The test functions FPT_TST.1/SSCD provides failure detection throughout the lifecycle.

375 **OT.SCD/SVD_Gen** (*SCD/SVD generation*) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1/SSCD and FIA_UAU.1/SSCD provide user identification and user authentication prior to enabling access to authorized functions. The SFR FDP_ACC.1/SCD/SVD_Generation_SFP_\ SSCD and FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin_SSCD, FMT_MSA.2/SSCD, and FMT_MSA.3/SSCD for static attribute initialization. The SFR FMT_MSA.4/SSCD defines rules for inheritance of the security attribute “SCD operational” of the SCD.

376 **OT.SCD_Unique** (*Uniqueness of the signature-creation data*) implements the requirement of practically unique SCD as laid down in [ALGO], which is provided by the cryptographic algorithms specified by FCS_CKM.1/SSCD.

377 **OT.SCD_SVD_Corresp** (*Correspondence between SVD and SCD*) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algo-

rithms specified by FCS_CKM.1/SSCD to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent_SSCD ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1/SSCD and by FMT_MSA.4/SSCD allow R.Admin to modify the default value of the security attribute SCD Identifier.

378 **OT.SCD_Secrecy** (*Secrecy of signature-creation data*) is provided by the security functions specified by the following SFR. FCS_CKM.1/SSCD ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.
The security functions specified by FDP_SDI.2/Persistent_SSCD ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). SFR FPT_EMSEC.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD-

379 **OT.Sig_Secure** (*Cryptographic security of the digital signature*) is provided by the cryptographic algorithms specified by FCS_COP.1/SSCD, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent_SSCD corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature-creation.

380 **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) is provided by an SFR for identification authentication and access control. FIA_UAU.1/SSCD and FIA_UID.1/SSCD ensure that no signature generation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin_SSCD and FMT_MTD.1/Signatory_SSCD manage the authentication function. SFR FIA_AFL.1/SSCD provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS_SSCD ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process).

381 The security functions specified by FDP_ACC.1/Signature-creation_SFP_SSCD and FDP_ACF.1/Signature-creation_SFP_SSCD provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory_SSCD, FMT_\ MSA.2/SSCD, FMT_MSA.3/SSCD and FMT_MSA.4/SSCD. The SFR FMT_SMF.1/ SSCD and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1/SSCD restricts the ability to enable the signature-creation function to the signatory. FMT_MSA.1/Signatory_SSCD restricts the ability to modify the security attributes SCD operational to the signatory.

382 **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS_SSCD require that the DTBS/R has not been altered by the TOE.

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

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

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

6.3.2 Rationale for SFR's Dependencies

386 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.

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

No.	SFR-component from the ST	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 56 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 57 FCS_CKM.4
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/SYM_ICAO-EAC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_CA FCS_CKM.4
10	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
11	FCS_COP.1/MAC_ICAO-EAC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1/DH_CA FCS_CKM.4
12	FCS_RND.1	No dependencies	n.a.
13	FIA_AFL.1/eID-PIN_Suspending	FIA_UAU.1	FIA_UAU.1/PACE

No.	SFR-component from the ST	Dependencies assumed	Fulfilled by SFR
14	FIA_AFL.1/eID-PIN_Blocking	FIA_UAU.1	FIA_UAU.1/PACE
15	FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1/PACE
16	FIA_API.1/CA	No dependencies	n.a.
17	FIA_API.1/ICAO-EAC	No dependencies	n.a.
18	FIA_APO.1/PA_PACE-Pass	No dependencies	n.a.
19	FIA_UID.1/PACE	No dependencies	n.a.
20	FIA_UID.1/Rightful_Terminal	No dependencies	n.a.
21	FIA_UID.1/ICAO-EAC	No dependencies	n.a.
22	FIA_UAU.1/PACE	FIA_UID.1	FIA_UID.1/PACE
23	FIA_UAU.1/Rightful_Terminal	FIA_UID.1	FIA_UID.1/Rightful_Terminal
24	FIA_UAU.1/ICAO-EAC	FIA_UID.1	FIA_UID.1/ICAO-EAC
25	FIA_UAU.4	No dependencies	n.a.
26	FIA_UAU.4/ICAO-EAC	No dependencies	n.a.
27	FIA_UAU.5	No dependencies	n.a.
28	FIA_UAU.5/ICAO-EAC	No dependencies	n.a.
29	FIA_UAU.6	No dependencies	n.a.
30	FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
31	FDP_ACF.1/TRM	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/TRM justification see page 76
32	FDP_RIP.1	No dependencies	n.a.
33	FTP_ITC.1/PACE	No dependencies	n.a.
34	FTP_ITC.1/CA	No dependencies	n.a.
35	FAU_SAS.1	No dependencies	n.a.
36	FMT_SMF.1	No dependencies	n.a.
37	FMT_SMR.1	FIA_UID.1	FIA_UID.1/PACE, FIA_UID.1/Rightful_Terminal see also Application Note 69
38	FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
39	FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
40	FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
41	FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
42	FMT_MTD.1/CVCA_INI	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
43	FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

No.	SFR-component from the ST	Dependencies assumed	Fulfilled by SFR
44	FMT_MTD.1/DATE	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
45	FMT_MTD.1/PA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
46	FMT_MTD.1/SK_PICC	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
47	FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
48	FMT_MTD.1/eID-PIN_Resume	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
49	FMT_MTD.1/eID-PIN_Unblock	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
50	FMT_MTD.1/eID-PIN_Activate	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
51	FMT_MTD.3	FMT_MTD.1	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE
52	FPT_EMSEC.1	No dependencies	n.a.
53	FPT_FLS.1	No dependencies	n.a.
54	FPT_TST.1	No dependencies	n.a.
55	FPT_PHP.3	No dependencies	n.a.

Table 18: Dependencies between the SFRs

388 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.

389 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.

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

No.	SFR-component from the ST	Dependencies assumed	Fulfilled by SFR
56	FCS_CKM.1/SSCD	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/SSCD FCS_CKM.4
57	FCS_COP.1/SSCD	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/SSCD FCS_CKM.4
58	FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD

No.	SFR-component from the ST	Dependencies assumed	Fulfilled by SFR
59	FDP_ACC.1/Signature_Creation_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/Signature_Creation_SFP_SSCD
60	FDP_ACC.1/SVD_Transfer_SFP_SSCD	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP_SSCD
61	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
62	FDP_ACF.1/Signature_Creation_SFP_SSCD	FDP_ACF.1 FMT_MSA.3	FDP_ACC.1/Signature_Creation_SFP_SSCD FMT_MSA.3/SSCD
63	FDP_ACF.1/SVD_Transfer_SFP_SSCD	FDP_ACF.1 FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP_SSCD FMT_MSA.3/SSCD
64	FDP_SDI.2/Persistent_SSCD	No dependencies	n.a.
65	FDP_SDI.2/DTBS_SSCD	No dependencies	n.a.
66	FIA_AFL.1/SSCD	FIA_UAU.1	FIA_UAU.1/SSCD
67	FIA_UAU.1/SSCD	FIA_UID.1	FIA_UID.1/SSCD
68	FIA_UID.1/SSCD	No dependencies	n.a.
69	FMT_MOF.1/SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1
70	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 FMT_SMF.1/SSCD
71	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 FMT_SMF.1/SSCD
72	FMT_MSA.2/SSCD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD FMT_SMR.1
73	FMT_MSA.3/SSCD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin_SSCD, FMT_MSA.1/Signatory_SSCD FMT_SMR.1
74	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
75	FMT_MTD.1/Admin_SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1
76	FMT_MTD.1/Signatory_SSCD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1/SSCD FMT_SMR.1
77	FMT_SMF.1/SSCD	No dependencies	n.a.
78	FMT_SMR.1	FIA_UID.1	FIA_UID.1/SSCD
79	FPT_PHP.1/SSCD	No dependencies	n.a.

Table 19: Dependencies between the SFRs required by [SSCDPP]

391 The dependency analysis given in the SSCD PP [[SSCDPP] 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

392 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.

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

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

395 The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined 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 4, entry 'Attacker'). This decision represents a part of the conscious security policy for the RP_Card required by the RP_Card issuer and reflected by the [RPCARDPP].

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

397 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. [RPCARDPP, Table 15]).

6.3.4 Security Requirements – Internal Consistency

398 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.

399 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.

400 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

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

402 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 RP_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

403 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

404 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

405 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 and FCS_COP.1/SYM_\ICAO-EAC for a EIS-AIP-BAC terminal giving confidentiality by data encryption/ decryption and FCS_COP.1/CMAC or FCS_COP.1/MAC_ICAO-EAC for a EIS-AIP-BAC terminal 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

406 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 based on PACE, FIA_UID.1/ICAO-EAC, FIA_UAU.1/ICAO-EAC for EIS-AIP-EAC terminals, and FIA_UID.1/SSCD, FIA_UAU.1/SSCD for the eSign application) and also for 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.

407 The TOE itself must also be authenticated, which is supported by FIA_API.1/CA and FIA_API/ICAO-EAC for EIS-AIP-EAC terminals. The ePassport application can be authenticated by Passive Authentication supported by FIA_APO.1/PA_PACE-Pass. The Requirements laid down in FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 (and the corresponding iterations FIA_UAU.4/ICAO-EAC, FIA_UAU.5/ICAO-EAC for EIS-AIP-EAC terminals supporting version 1 algorithms) concerns the protocol data, prevents the re-use of authentication data and how a security state, e.g. a specified role (FMT_SMR.1) of an identified and authenticated user or device, is achieved and maintained.

408 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.

409 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.

410 The identification and authentication of the RP_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).

411 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 RP_Card and the terminal. As the authentication state is left, the session keys can not be used anymore (FCS_CKM.4).

7.4 Audit

412 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

413 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).

414 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.

415 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).

416 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

417 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

418 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) 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).

419 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.

420 CAN, MRZ or eID-PUK represent non-blocking authentication data, which is used to establish a secure channel. No additional access rights are granted after sucessfully executed PACE protocol. To avert the inconspicuous skimming of the TOE, the initial

PACE protocol must be restarted if any failure has been detected (FIA_AFL.1/PACE). Due to the reaction time a brute force attack would require days even for the short valued CAN. Therefore increasing the reaction time ist not necessary.

421 The eID-PIN can be resumed (FMT_MTD.1.1/eID-PIN-Resume) by the RP_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 RP_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).

422 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).

423 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).

424 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

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

426 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.

427 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).

428 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).

429 This functionality is supported by the entire class FMT.

7.9 TOE SFR Statements

430 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.

431 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.

432 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.

433 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.

434 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

435 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.

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

437 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.

438 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.

439 FCS_COP.1/SYM_ICAO-EAC The Triple DES is not classified as secure as the AES due to the smaller key length. Taking in account the fact that this algorithm is used only in the case of backward compatibility for EIS-AIP-BAC terminals and that the security level is higher that 100 bit the TDEA can be used until the EIS-AIP-BAC terminals are phased out (see also Application Note 53 of [RPCARDPP]).

440 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.

441 FCS_COP.1/MAC_ICAO-EAC The Retail-MAC is used for secure messaging and is restricted to data from DG3 and DG4 for EIS-AIP-BAC terminals only. Due to the low data exchange the Retail MAC remains secure for this application (see also Application Note 54 of [RPCARDPP]).

442 FCS_RND.1 The randomness of values for challenges or ephemeral or permanent keys be guaranteed by the underlying hardware TSF. To achieve the SOF “high” the generated data must have sufficient entropy. This is fulfilled automatically if the random number generator is certified as P2 according [AIS31]. To avoid any non-uniformity and additional cryptographic post-processing for PACE nonces is applied.

443 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.

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

445 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. If any authentication failure for the non-blocking authentication data (CAN, MRZ, eID-PUK) has been detectected during the PACE protocol, the TSF blocks the protocol and require a restart of the PACE. Because MRZ and eID-PUK carry enough entropy the minimal reaction time is sufficient to prevent a brute force attack with attack potential beyound high. Even for the case the CAN is used, this reaction time prevents the tracing of the card, since a brute force attack requires some days of permanent access to the TOE.

446 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.

447 FIA_APO.1/PA_PACE-Pass: The Passive Authentication making evident the authenticity/origin of data stored in the *ePassport* application by verifying the Document Security Object (SO_D) up to CSCA. 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 origin of *ePassport* application. Independent of the result of Passive Authentication, secure messaging is continued using the previously established session keys.

448 FIA_UID.1/PACE, FIA_UID.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.

449 FIA_UAU.5, FIA_UAU.5/ICAO-EAC: 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.

450 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.

451 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, Part 3, Annex C, Table 20] 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.

452 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.

453 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]).

454 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.

455 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.

456 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).

457 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.

458 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.

459 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 RP_Card holder.

460 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.

461 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.

462 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.

463 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 correspondig status code, that an error occurred. During opeartions the integrity check will be provided by the hardware.

464 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.

465 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.

466 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.

467 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.

468 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.

469 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.

470 FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE: The intial Personalization data from the Issuing Branch is

471 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.

472 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.

473 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.

474 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.

475 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.

476 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.

477 FMT_SMR.1, 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.

478 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.

479 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.

480 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.

481 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”.

482 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”.

483 FMT_MTD.1/Admin_SSCD: During SCD/SVD generation the initial RAD (reference authentication data) is generated by the CSP (S.Admin). This special RAD value (Transport-PIN) can never be used for creating digital signatures.

484 FMT_MTD.1/Signatory_SSCD: Only the Signatory, authenticated as the RP_Card holder can modify the initial RAD (Transport-PIN). After the Transport-PIN value is changed by the Signatory, the SCD is set to “operational”.

485 FPT_EMSEC.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.

486 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

487 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.

488 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.

489 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

490 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

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

Relevant:

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

  Cryptographic support includes 3DES, AES, RSA (not relevant), EC (not relevant), SHA-2 (SHA-256 and SHA512 – both not relevant), TRNG (relevant).

Not relevant:

7.10.2 Compatibility: TOE Security Environment

Assumptions

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

Assumptions of the Composite ST: None

Assumptions 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].

493 The identified here Objectives are related to OE.Passive_Auth_Sign and OE.Personalization, that ensure the establishment of the correct identity of the RP_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 RP_Card holder engage a CSP to make it available after certificate creation.

Assumptions of the Hardware PP ([PP0035]):

494 A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization) is relevant until the Personalization of the hardware (TOE Initialization)

The assumption A.Process-Sec-IC covers the secure handling of the SC from the delivery by the hardware manufacturer to the developer until the completion of the TOE. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance families ALC_DEL and ALC_DVS. This assumption is no more required for Composite TOE and is therefore not included into this Composite ST.

495 A.Plat-Appl (Usage of Hardware Platform) is relevant during TOE development

The assumption A.Plat-Appl assumes that the Smartcard Embedded Software securely uses the hardware, taking into account the hardware user guidance and the hardware evaluation. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance family ADV_COMP. That corresponds to the achievement of the security objectives e.g. OT.EMSEC-Design, OT.Tamper-ID and OT.Tamper-Resistance in the TOE end usage. This assumption is not required for Composite TOE and is therefore not included into this Composite-ST.

496 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.

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

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

  Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). This assumption is covered by the Hardware's objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 "Development".

Threats

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

Threats of the Composite ST:

- T.Skimming no conflict
- T.Eavesdropping no conflict
- T.RP_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]

Threats of the hardware ST ([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.DTBS_Forgery and T.Sig_Forgery 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 and signature generation if the eSign Application becomes operational.

Threats of the hardware ST ([HWST]):

T.Mem-Access (Memory Access Violation)

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

Threats of the of the SSCD PP ([SSCDPP]):

- T.SCD_Divulg is related to signature creation data only and is not contradicting the threats of the Composite ST
- T.SCD_Derive is related to signature creation data only and is not contradicting the threats of the Composite ST
- T.Hack_Phys matches T.Phys-Tamper of the Composite ST
- T.SVD_Forgery is covered by T.Forgery and T.Eavesdropping of the Composite ST

- T.SigF_Misuse is covered by T.Abuse-Func of the Composite ST
- T.DTBS_Forgery is covered by T.Skimming and T. Forgery of the Composite ST
- T.Sig_Forgery is related to signature creation data only and is not contradicting the threats of the Composite ST

Organizational Security Policies

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

Organizational Security Policies of the Composite ST of the TOE:

- P.Pre-Operational covers P.Process-TOE of the hardware ST
- P.Terminal no conflict
- P.RP_Card_PKI no conflict
- P.Terminal_PKI no conflict
- P.Trustworthy_PKI no conflict

Organizational Security Policies of the Hardware ST:

- P.Add-Functions (Additional Specific Security Functionality) no conflict
  The TOE' hardware provides the following specific security functionality to the Smartcard Embedded Software: Advanced Encryption Standard, Triple Data Encryption Standard (not relevant), Rivest-Shamir-Adleman Cryptography (not relevant), Elliptic Curve Cryptography (not relevant), Secure Hash Algorithm SHA-2.
- P.Process-TOE ([PP0035]) is covered by P.Pre-Operational of the Composite ST

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

Security Objectives

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

Security Objectives for the Composite ST of the TOE:

- OT.Data_Integrity covers O.Add_Functions (AES) of the [HWST]
- OT.Data_Authenticity covers O.Add_Functions (AES) of the [HWST]
- OT.Data_Confidentiality covers O.Add_Functions (AES) of the [HWST]

- OT.Tracing no conflict
- OT.Chip_Auth_Proof no conflict
- OT.Prot_Abuse-Func covers O.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_Malfunction matches O.Malfunction from [PP0035]
- OT.Identification matches O.Identification from [PP0035]
- OT.Personalization no conflict

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.Prot_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.Add-Functions (Additional Specific Security Functionality)

  The hardware TOE provides the security functionalities Advanced Encryption Standard (AES) and Triple Data Encryption Standard (TDES) to the Smartcard Embedded Software, which is mapped OT.Data_Integrity, OT.Data_\ Authenticity and OT.Data_Confidentiality. The security functionality of Rivest-Shamir-Adleman algorithm, Elliptic Curve Cryptography and Secure Hash Algorithm is not used and therefore not relevant.
- O.MEM_ACCESS is mapped to T.MEM_ACCESS

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

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.Prot_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.EMSEC_Design is covered by OT.Prot_Inf_Leak and OT.Prot_Phys-Tamper
- OT.Tamper_ID is covered by OT.Prot_Phys-Tamper
- OT.Tamper_Resistance is covered by OT.Prot_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 RP_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.Card-Holder
- OE.DTBS_Protect is covered by OE.Card-Holder and OE.Terminal
- OE.Signatory is covered by OE.Card-Holder

The obligation for a CSP activating an eSign application is to supply the RP_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.

Security Requirements

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

Security Requirements of the Composite ST of the TOE:

- FCS_CKM.1/DH_PACE not relevant
- FCS_CKM.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/AES matches FCS_COP.1/AES of [HWST]
- FCS_COP.1/SYM_ICAO-EAC matches FCS_COP.1/DES of [HWST]
- FCS_COP.1/CMAC no conflicts
- FCS_RND.1 matches FCS_RNG.1 of [HWST]
- FIA_AFL.1/eID-PIN_Suspending no conflicts
- FIA_AFL.1/eID-PIN_Blocking 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
- FDP_ACC.1/TRM not relevant
- FDP_ACF.1/TRM not relevant
- FDP_RIP.1 no conflicts
- FTP_ITC.1/CA not relevant
- FAU_SAS.1 matches FAU_SAS.1 of [HWST]
- FMT_SMF.1 no conflicts
- FMT_SMR.1 not relevant
- FMT_LIM.1 matches FMT_LIM.1 of [HWST]
- FMT_LIM.2 matches FMT_LIM.2 of [HWST]
- FMT_MTD.1/INI_ENA not relevant
- FMT_MTD.1/INI_DIS not relevant
- FMT_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_EMSEC.1 is supported by the Security Feature SF_PS of the hardware ([HWST]) and the AVA_VAN.5 evaluation
- FPT_FLS.1 matches FPT_FLS.1 of [HWST]
- FPT_TST.1 no conflicts
- FPT_PHP.3 matches FPT_PHP.3 of [HWST]

Security Requirements of the hardware

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

Assurance Requirements

501 The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

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

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

7.10.3 Conclusion

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

7.11 Assurance Measures

505 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 0.

Development

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

Guidance documents

AGD_OPE.1	User Guidance TCOS RP_Card
AGD_PRE.1	Administrator Guidance TCOS RP_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 RP_Card
ALC_TAT.1, ALC_DVS.2	Development Tools and Development Security for TCOS RP_Card

Tests

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

Vulnerability assessment

AVA_VAN.5	Independent Vulnerability Analysis TCOS RP_Card

506 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.

507 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.

508 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.

509 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.

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

511 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

512 This is the unchanged chapter from [RPCARDPP], 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 RP_Card's chip to produce Terminal Certificates with the correct certificate effective date, see also [EACTR, Part 3, 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 an ST or 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 RP_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 RP_Card presenter as the RP_Card holder (using the secret eID-PIN[303]), (ii) updating a subset of data of the eID application and (iii) activating the eSign application. See also [EACTR, Part 1, 2.2 and Part 3, C.4].
Authenticity	Ability to confirm that the RP_Card itself and the data elements stored in were issued by the RP_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[304] 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 RP_Card using the Document Basic Access Keys drawn from printed MRZ data for reading the less-sensitive data (RP_Card document details data and biographical data) stored on the RP_Card (ePassport application only). See also [EACTR, Part 1, 2.4.1 and A]; also [ICAO9303-1].
Biographical data (biodata)	The personalized details of the RP_Card holder appearing as text in the visual and machine readable zones of and electronically stored in the RP_Card. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the RP_Card holder in the RP_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 on a label on the Identification Card) or dynamic (randomly chosen by the electronic RP_Card

303 the secret eID-PUK can be used for unblocking the eID-PIN and resetting the retry counter related

304 concretely, by a control officer

Term	**Definition**
	and displayed by it using e.g. ePaper, OLED or similar technologies), see [EACTR, Part 1, 2.3 and Part 2, 2.3].
Card Security Object (SO_C)	A RFC 3369 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the RP_Card (EF.CardSecurity, see [EACTR, Part 3, Annex A]) and carries the hash values of different Data Groups as defined in [EACTR, Part 3, Appendix A]. It shall also carry the Document Signer Certificate (C_{DS}) [EACTR, Part 3, 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 RP_Card issuer with respect to confirming correctness of user and TSF data stored in the RP_Card. The CSCA represents the country specific root of the PKI for the RP_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, Part 3, 2.1].
Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the RP_Card issuer with respect to protection of user data stored in the RP_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, Part 3, 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, Part 3, 2.1].
CV Certificate	Card Verifiable Certificate according to [EACTR, Part 3, 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 RP_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: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the ePassport application of the RP_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 RP_Card/Chip and Document Security Objects stored on the RP_Card for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR, Part 1, 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, Part 3, 2.2.2]. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the do-

Term	**Definition**
	mestic CVCA being run by the RP_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 RP_Card issuer und a foreign CVCA ensuring enforcing the RP_Card issuer's privacy policy[305]).
Eavesdropper	A threat agent reading the communication between the RP_Card and the Service Provider to gain the data on the RP_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, Part 2, 2.1.2].
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, Part 2, 2.1.1].
eSign application	A part of the TOE containing the non-executable data needed for generating advanced or qualified electronic signatures on behalf of the RP_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 RP_Card holder is required. The eSign application is optional: it means that it can optionally be activated[306] on the RP_Card by a Certification Service (or on his behalf) using the ATT with an appropriate authorization level. See [EACTR, Part 2, 2.1.3].
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.
RP_Card (electronic)	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally)
RP_Card holder	The rightful/legitimated holder of the electronic ID Card for whom the issuing authority personalized the ID Card.
RP_Card issuer (issuing authority)	Organization authorized to issue an electronic Identity Card to the RP_Card holder
RP_Card presenter	person presenting the RP_Card to a terminal and claiming the identity of the RP_Card holder

305 Existing of such an agreement may be technically reflected by means of issuing a $C_{CVCA\text{-}F}$ for the Public Key of the foreign CVCA signed by the domestic CVCA.

306 '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]
Initialization Data	Any data defined by the RP_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 RP_Card presented to it by an RP_Card presenter and verifying its authenticity as the RP_Card holder. See also [ICAO9303-1].
Inspection system (EIS)	A technical system being used by an authority[307] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data of the RP_Card presenter with the stored biometrical data of the RP_Card holder). The specification [EACTR, Part 2, 2.2 and Part 3, 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 RPCARDPP) is commensurate with the Extended Inspection System (EIS) as defined in [EACPP3.1][308].
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The RP_Card's chip is an integrated circuit.
Integrity	Ability to confirm the RP_Card and its data elements stored upon have not been altered from that created by the RP_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 RP_Card).
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the RP_Card Manufacturer completing the IC to the RP_Card. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC

307 concretely, by a control officer

308 please note that an Extended Inspection System also covers the General Inspection Systems (GIS) in the sense of [EACPP3.1]

Term	Definition
	Manufacturer and RP_Card Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [EACTR, Part 3, C.1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorization Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE Terminal (PCT)	A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the RP_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, Part 2, 2.3, 3.2, and Part 1, Table 3 and A.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, Part 1, 1.1].
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [EACTR, Part 2, 3.2]. 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 RP_Card holder. PIN is a blocking password; see [EACTR, Part 1, 2.3 and Part 2, 2.3].
Personalization	The process by which the individual-related data (biographic and biometric data, signature key pair(s) for the eSign application) of the RP_Card holder are stored in and unambiguously, inseparably associated with the RP_Card.
Personalization Agent	An organization acting on behalf of the RP_Card issuer to personalize the RP_Card for the RP_Card holder by some or all of the following activities: (i) establishing the identity of the RP_Card holder for the biographic data in the RP_Card[309], (ii) enrolling the biometric reference data of the RP_Card holder[310], (iii) writing a subset of these data on the physical Identification Card (optical personalization) and storing them in the RP_Card (electronic personalization) for the RP_Card holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card/Chip Security Object and the Document Security Object (ePassport) 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 CSP actions providing Personalization Data to the CSP.
PIN Unblock Key (PUK)	A long secret password being only known to the RP_Card holder. The PUK is a non-blocking password; see [EACTR, Part 2, 2.3].
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 RP_Card and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalized RP_Card's chip	RP_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 RP_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

309 relevant for the ePassport, the eID and the eSign applications

310 relevant for the ePassport application

Term	Definition
	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, Part 2, 2.1.2].
Restricted Identification	Restricted Identification aims providing a temporary RP_Card identifier being specific for a terminal sector (pseudo-anonymization) and supporting revocation features (see Part 3, 2.6, and Part 2, 3.5 of [EACTR]. The security status of RP_Card is not affected by Restricted Identification.
Rightful equipment (rightful terminal or rightful RP_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 RP_Card can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for an RP_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 RP_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, Part 1, 2.2 and Part 3, 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 RP_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 RP_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 RP_Card gathered by inconspicuous (for the RP_Card holder) recognizing the RP_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 RP_Card	RP_Card material prepared to produce a personalized RP_Card containing an initialized and pre-personalized RP_Card's chip.
User Data	All data (being not authentication data) stored in the context of the applications of the RP_Card as defined in [EACTR] and 1. being allowed to be *read out or written* solely by an authenticated terminal (in the sense of [EACTR], Part 2, 2.2) respectively 2. being allowed to be *used* solely by an authenticated terminal (in the sense of [EACTR, Part 2, 2.2]) (the private Restricted Identification key; since the Restricted Identification according to [EACTR, Part 2, 3.5] represents just a functionality of the RP_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 RP_Card holder (the private signature key within the eSign application); from this point of view, the private signature key of the RP_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, Part 2, 2.2]
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', hence this is adopted here)
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, Part 2, 2.2])
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, Part 2, 2.2]
SVD	Signature Verification Data, please refer to [SSCDPP]
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functions
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data, please refer to [SSCDPP]

References

[AIS31]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Version 1 vom 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ALGO]
Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, 30.12.2011, Veröffentlicht am 18.01.2012 im Bundesanzeiger Nr. 10, S. 243

[BACPP3.1]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, BSI-PP-0055, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-29

[BACCR] Certification Report of the TCOS Residence Permit Card (BAC)
BSI-DSZ-CC-0836-2013: TCOS Residence Permit Card (BAC) Version 1.1 Release 1/ SLE78CLX1440P, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013-09-12

[BACST] Security Target TCOS Residence Permit Card (BAC)
Specification of the Security Target TCOS Residence Permit Card (BAC) Version 1.1 Release 1/SLE78CLX1440P, Version 1.1.1/20130912, T-Systems International GmbH, 2013-09-12

[CC]
Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model; Version 3.1 R4, Sept. 2012, CCMB-2012-09-001,
Part 2: Security functional components; Version 3.1 R4, Sept. 2012, CCMB-2012-09-002,
Part 3: Security assurance components; Version 3.1 R4, Sept. 2012, CCMB-2012-09-003

Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 R4, Sept. 2012, CCMB-2012-09-004

[EACPP2.3]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.2, BSI-PP-0026, 2006-09-07

[EACPP3.1]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.10, BSI-PP-0056, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25

[EACTR1.11]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008-02-21

[EACTR2.03]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-03-24

[EACTR]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Part 1, 2, 3, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03

[ECARDTR]
Technische Richtlinie TR-03116-2 für die eCard-Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, Stand 2011, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011

[ECCTR]
Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06

[EURPS]
EU – Residence permit Specification, Annex II.a to Commission Decision C(2008), version 1.0, 20.08.2008

[FIPS46]
Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), July 1977, Reaffirmed October 1999

[FIPS180]
Federal Information Processing Standards Publication FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS), February 2004

[FIPS186]
Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), June 2009

[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-0813-2012 for Infineon Technologies Smart Card IC (Security Controller) M7820 A11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06

[HWST] Security Target of the underlying hardware platform
Security Target M7820 A11, Version 1.5, Infineon Technologies AG, Chipcard and Security, Evaluation Documentation, 2012-05-07

[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

[PACEPassPP]
CC Protection Profile: Electronic Passport using Standard Inspection Procedure with PACE, BSI-CC-PP-0068, Version 0.92, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0068-2010, 2010-04-30

[RFC5639]
M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[RPCARDPP]
CC Protection Profile: Electronic Residence Permit Card (RP_Card PP), Version 1.00, BSI-PP-0069, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-08-13

[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

[ISO9797]
ISO 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO, 2005-01-04

[ISO14443]
ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

[ISO15946]
ISO 15946, Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002

[PP0035]
Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007

[SP800-38B]
Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

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

[TCOSADM]
TCOS Residence Permit Card Version 1.1 Release 1, Administrator's Guidance Version 1.0, T-Systems International GmbH, 2013