LIFE IS FOR SHARING.

Specification of the Security Target TCOS ID Version 3.0 Release 1/P71

Version: 3.0.1/20230327

Document ID:	CD.TCOS.ASE
Filename:	ASE TCOS ID 3.0.1 (NXP).docx
Date:	27.03.2023
Version:	3.0.1
Hardware Base:	P71
Author:	Ernst-G. Giessmann, Markus Blick
Confidentiality Level:	**Public**

History

Version	Date	Remark
3.0.1	2023-03-27	Final document

Contents

Contents **3**
1 ST Introduction **5**
1.1 ST Reference 5
1.2 TOE Reference 5
1.3 TOE Overview 5
1.3.1 TOE security features for operational use 8
1.3.2 TOE Type 8
1.3.3 File System of the TOE 9
1.3.4 Life Cycle Phases Mapping 9
1.3.5 Non-TOE hardware/software/firmware 12
1.3.6 TOE Boundaries 13
1.3.7 Conformance to eIDAS 13
2 Conformance Claim **14**
2.1 CC Conformance Claims 14
2.2 PP Claims 14
2.3 Package Claims 15
2.4 Conformance Claim Rationale 15
3 Security Problem Definition **17**
3.1 Assets and External Entities 17
3.2 Threats 20
3.3 Organizational Security Policies 26
3.4 Assumptions 30
4 Security Objectives **32**
4.1 Security Objectives for the TOE 32
4.2 Security Objectives for the Operational Environment 38
4.3 Security Objective Rationale 43
5 Extended Components Definition **46**
5.1 FAU_SAS Audit data storage 46
5.2 FCS_RND Generation of random numbers 46
5.3 FIA_API Authentication Proof of Identity 47
5.4 FMT_LIM Limited capabilities and availability 47
5.5 FPT_EMS TOE Emanation 48
6 Security Requirements **50**
6.1 Security Functional Requirements for the TOE 50
6.1.1 Overview 51
6.1.2 Class FAU Security Audit 54
6.1.3 Class FCS Cryptographic Support 55
6.1.4 Class FIA Identification and Authentication 70
6.1.5 Class FDP User Data Protection 86
6.1.6 Class FMT Security Management 101
6.1.7 Class FPT Protection of the Security Functions 120

6.1.8 Class FTP Inter-TSF trusted channel 126
6.2 Security Assurance Requirements for the TOE 130
6.3 Security Requirements Rationale 130
6.3.1 Rationale for SFR's Dependencies 130
6.3.2 Security Assurance Requirements Rationale 133
7 TOE Summary Specification 134
7.1 Identification and Authentication 134
7.2 Secure Communication 136
7.3 Secure Key Pair Generation 137
7.4 Signature creation 137
7.5 Access Control for stored objects 138
7.6 Update in the Field 139
7.7 Reliability of stored information 140
7.8 Statement of Compatibility 141
7.8.1 Relevance of Hardware TSFs 141
7.8.2 Security Requirements 141
7.8.3 Security Objectives 144
7.8.4 Conclusion 146
7.9 Assurance Measures 146
Appendix Glossary and Acronyms 148
References 149

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 ID Version 3.0 Release 1/P71
TOE:	TCOS ID Version 3.0 Release 1/P71
Sponsor:	Deutsche Telekom Security GmbH
Editor(s):	Deutsche Telekom Security GmbH
CC Version:	3.1 (Revision 5)
Assurance Level:	EAL4 augmented.
General Status:	Final Document
Version Number:	3.0.1
Date:	2023-03-27
Certification ID:	BSI-DSZ-CC-1188
Keywords:	ICAO, PACE, EAC, Extended Access Control, ID-Card, Machine Readable Electronic Document, TCOS

1.2 TOE Reference

3 This Security Target refers to the Product “TCOS ID Version 3.0 Release 1/P71” (TOE) of Deutsche Telekom Security GmbH for CC evaluation.

1.3 TOE Overview

4 The Target of Evaluation (TOE) addressed by this Security Target is a smart card with a contact-less interfaces programmed according to [EACTR]. The smart card contains at least one application described in the following. In this ST the TOE as a whole is also called Electronic Document.

5 Here, an application is a collection of data (data groups) and their access conditions. We mainly distinguish between common user data, and sensitive user-data. Depending on the protection mechanisms involved, these user data can further be distinguished as follows:

- EAC1-protected data: Sensitive user data protected by EAC1 (cf. [EACTR-1]),
- EAC2-protected data: Sensitive user data protected by EAC2 (cf. [EACTR-2]), and
- all other (common) user data. Other user data are protected by Password Authenticated Connection Establishment (PACE, cf. also [EACTR-2]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE.

6 *Application Note 1:* Due to migration periods both PACE and Basic Access Control (BAC) according to [ICAO9303] were supported by MRTD products in the past. Starting 1 January 2018, eMRTD chips implementing PACE only also comply with [ICAO9303]. This TOE does not support BAC.

7 In addition to the above user data, there is also data required for TOE security functionality (TSFs). Such data is necessary to execute the access control protocols, to verify integrity and authenticity of user data, or to generate cryptographic signatures.

8 Applications considered in [EACTR-1] and [EACTR-2] are

- an electronic passport (ePass[1]) application,
- an electronic identity (eID) application, and
- a signature (eSign) application.

9 Deutsche Telekom Security GmbH implemented all these applications in the TOE. They are subject of CC Evaluation.

10 The terminology used here follows [MREDPP, Table1], where an appropriate translation table of the identifiers used in different relevant Protection Profiles is given.

11 According to the Technical Guideline TR-03110 (cf. [EACTR-1, 2.1.1]) the ePass application supports Passive Authentication, Password Authenticated Connection Establishment (PACE) with CAN and MRZ as parts of the Standard and General Inspection Procedure, Terminal and Chip Authentication P.CS 2 and Version 3 as required in the General Inspection Procedure and also Basic Access Control (BAC). The reason for the requirement to include BAC was the wanted compliance with [ICAO9303] (cf. [EACTR-2, 1.1]). However, since the eighth edition of [ICAO9303] eMRTD chips implementing PACE only also comply to [ICAO9303]. Therefore, BAC in combination with Extended Access Control (EAC) with Chip and Terminal Authentication Version 1 are removed in this version of the security target.

12 The ePass or eID Applications 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]).

13 For the ePass Application, the electronic document holder can control the access to his user data by conscious presenting his document to authorities[2] (CAN or MRZ authentication as specified in [EACTR-1, 3.3]).

14 For the eID Application, the electronic document holder can control the access to his user data by inputting his secret PIN or by conscious presenting his document to the authorities[3].

15 For the eSign application, the electronic document holder can control the access to the digital signature functionality by conscious presenting his document to a Service Provider and using his secret Verification Authentication Data for this application: eSign-PIN[4].

16 *Application Note 2:* 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 organizationally get different values of the respective secret PINs (PIN and eSign-

1 The notation of this application is different in the references; both *ePass* and *ePassport* are used. In this ST they are used synonymously, too.

2 CAN or MRZ user authentication, see [EACTR-1, sec. 2.3]

3 PIN or CAN user authentication, see [EACTR-1, sec. 2.3 and Part 2, sec. 2.3]

4 CAN and eSign-PIN (VAD as specified in [SSCDPP, sec. 3.2.3.5]).), user authentication, see [EACTR-2, sec. 2.3]

PIN). It is especially important, since qualified electronic signatures will be generated by the eSign Application. For security reasons this policy will not be enforced by the TOE.

17 The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure (cf. [ALGO]). The security parameters of these algorithms must be selected by the electronic document issuer according to the Organizational Security Policies, e.g. P.Personalization [EAC1PP] or P.QSign [ALGO]. The TOE supports the standardized domain parameters mentioned in [RFC5639] (key length 256, 320, 384 and 512 bit), and the NIST P-256 curve mentioned in [EACTR-3, A.2.1.1] (with key length 256 bit) including the corresponding hash functions. PACE and hence the General Inspection Procedure require the use of AES. A more detailed description is given in the Administrator Guidance [TCOSGD].

18 The electronic document is integrated into a plastic, optically and machine readable counterpart of the electronic document. Note that this is not part of the TOE.

19 The hardware may be relevant in some context, and if so, the TOE will be identified in more detail as “TCOS ID Version 3.0 Release 1/P71”, otherwise the shorter notion “TCOS ID Version 3.0 Release 1” will be used, indicating that this context may be applicable to any realization regardless which hardware base is used. Note that the hardware base is identified as P71D600.

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

21 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [MREDPP] and the Life Cycle Model required by [ICPP] will be shown in chap. 1.3.4.

22 The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (Card Operating System, COS) including configuration and initialization data related to the security functionality of the chip,
- the selected Applications implemented in the file-system to be installed, and
- the associated guidance documentation including description of the file system installation procedure.

23 The components of the TOE are therefore the hardware (IC) and the operating system TCOS (OS) ready for initialization with a selected dedicated object system. The TOE Design Specification gives a detailed description of the parts of TOE.

24 The dedicated object systems (file systems) are specified in detail in the Admin Guidance. All they support all security functionality and mechanisms described within the ST. After initialization and during personalization, applications (data groups) required for the intended functionality and mechanisms and their access rights are created. Creation of the applications (i.e. the ISO7816-4 conforming file structure) including data groups and their access rights) is subject to a limited availability and limited capability policy defined in the family FMT_LIM. In particular, the loader ensures that creation or alteration of the file system is not possible after the manufacturing phase (this excludes populating data groups with values, as is done in the personalization phase). This is necessary for the manufacturer to use a single IC for different configurations.

25 *Application Note 3*: Since parts of the contactless interface, e.g. the antenna, may have impact on specific aspects of vulnerability assessment and thus are security relevant,

these parts are considered as a part of the TOE. The decision upon this was made by the certification body in charge. Further details are considered in the ALC documentation.

26 The Guidance documentation ([TCOSGD]) provides further requirements for the manufacturer and security measures required for protection of the TOE until reception by the end-user.

1.3.1 TOE security features for operational use

27 The TOE here has all security features of the TOE defined in [MREDPP]. In addition, it allows updating the TOE software during the life-cycle phase 4 “Operational Use” according to [MREDONPP].

28 The following TOE security features are the most significant for its operational use. The TOE ensures that

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the electronic document according to the access rights of the terminal,
- the electronic document holder can control access by consciously presenting his electronic document and/or by entering his secret PIN,
- authenticity and integrity of user data can be verified,
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided,
- inconspicuous tracing of the electronic document is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created.

29 For further details, refer to the chapter 6 “Security Requirements” and chapter 7 TOE Summary Specification.

1.3.2 TOE Type

30 The TOE’s type addressed by this ST is according to [MREDPP] a smart card programmed according to [EACTR]. With the eSign Application the TOE implements a Secure Signature Creation Device according to Regulation (EU) No 910/2014 and the corresponding Implementing Decision [eIDAS].

31 The TOE type definitions of the claimed PPs ([EAC1PP], [EAC2PP], [SSCDPP]) differ slightly. It is shown in the Protection Profile [MREDPP] that these differences do not violate consistency. It will not be repeated here. To avoid renaming in this ST all the notations of the different PPs are taken over here.

32 The typical life cycle phases for the current TOE type are development, manufacturing, card issuing and operational use. The life cycle phase development includes development of the IC itself and IC embedded software. Manufacturing includes IC manufacturing and smart card manufacturing, and installation of a card operating system. Card issuing includes completion of the operating system, installation of the smart card applications and their electronic personalization, i.e. tying the application data up to the electronic document holder.

33 Operational use of the TOE is explicitly in the focus of the Protection Profile [MREDPP]. Nevertheless, some TOE functionality is already available in the manufacturing and the

card issuing life cycle phases. Therefore it is also considered by the Protection Profile [MREDPP] and this ST.

1.3.3 File System of the TOE

34 The TOE is configured with one of the dedicated file systems during life cycle phase 2 “Manufacturing”. Depending on the intended use, the file system of a desired configuration may not contain all applications listed in this ST. Although not all data groups will be present, all mechanisms, such as e.g., access controls and cryptographic operations described in the SFRs of this ST are implemented in these products too. The corresponding security requirements are fulfilled as soon as the application is available.

35 The available Major Configurations of the file system related to this ST are described in detail in other documents [TCOSGD]. They do not differ in security-relevant ways. For example, the product configured as *Passport* provides the same security functionality of an electronic travel document as the product configured as *ID Document*. Though the latter can be used as a *Qualified Signature Creation Device*, this has no impact on the security functionality of a *Passport*, not providing this functionality.

36 The two Major Configurations of the TOE in this Security Target, which differ only in the description of the object system, are:

- *Passport*: user data stored in an ICAO-compliant ([ICAO9303]) ePass Application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.
- *ID Document*: user data stored in an ICAO-compliant ePass application protected by PACE and EAC1/EAC2. Additional user data are stored in [EACTR-2] conformant eID and [SSCDPP] conformant eSign Applications, and are protected by EAC2.

37 Depending on the Configuration additionally the eSign Application can be already activated by a Certification Service Provider. The user data of the eSign Application are protected by PACE/EAC2.

1.3.4 Life Cycle Phases Mapping

38 Following the Protection Profile BSI-CC-0084 [ICPP, sec. 1.2.3] the life cycle phases of a smart card 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 6 is sub-divided in the phases 6.1 Installation and 6.2 Personalization)
Phase 7: Operational Use

39 In the following the phases of the Protection Profile BSI-CC-0084 are integrated but not named ‘phases’ but ‘steps’ to avoid ambiguity.

40 *Application Note 4:* The Protection Profile [MREDPP] also uses a subdivision of the phases into seven steps, referencing to BSI-CC-0084. But the steps 1 and 2 in [MREDPP] are exchanged compared to BSI-CC-0084. The following life cycle description uses the same order as in [MREDPP].

41 According to the Protection Profile [MREDPP], the TOE life cycle is described in terms of the following four life cycle phases, divided in steps.

Life cycle phase 1 “Development”

42 *Step 1*: The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC dedicated software and the guidance documentation associated with these TOE components.

43 *Step 2:* The software developer 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 electronic document application(s) and the guidance documentation associated with these TOE components.

44 The manufacturing documentation of the IC including the IC dedicated software and the embedded software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC embedded software in the non-volatile programmable memories, the application(s), and the guidance documentation is securely delivered to the electronic document manufacturer.

45 This life cycle phase steps cover exactly phase 1 and phase 2 of [ICPP].

Life cycle phase 2 “Manufacturing”

46 *Step 3*: In a first step, the TOE integrated circuit is produced. The circuit contains the electronic document’s chip dedicated software, and the parts of the electronic document’s chip embedded software in the non-volatile memory. The IC manufacturer writes IC identification data onto the chip in order to track and control the IC as dedicated electronic document material during IC manufacturing, and during delivery to the electronic document manufacturer. The IC is securely delivered from the IC manufacturer to the electronic document manufacturer.

47 *Step 4* (optional): The IC may be delivered as a module or a packaged component, combined with hardware for the contactless interface.

48 *Step 5*: The electronic document manufacturer

- if necessary, adds the IC embedded software, or parts of it in the non-volatile programmable memories, e. g. EEPROM or FLASH,

49 This step is called *Completion,* and the one and only one user of the TOE in this stage is the *Completion Agent* acting as manufacturer. After Completion the Operating System cannot be changed anymore except by functionalities described in the TOE SFRs with the iteration ‘/UPD’. The access protocols and the TSF are ready to use.

50 *Step 6.1:* The electronic document manufacturer

- creates the application(s), and
- equips the electronic document’s chip with pre-personalization data.

51 This step is called *Initialization*, the one and only one user of the TOE in this stage is the *Initializer*. Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), and elementary files (EFs) according to [ISO7816]. The keys and authentication data for Installation are delivered securely to the Installation Agent.

52 After *Initialization,* the electronic document is ready for import of user data (Personalization).

53 The pre-personalized electronic document together with the IC identifier is securely delivered from the electronic document manufacturer to the *Personalization Agent*. The elec-

tronic document manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent. The authentication data for personalization is delivered securely to the Personalization Agent.

54 This life cycle phase corresponds to the IC life cycle phases 3, 4, 5 and 6 of [ICPP], or more precisely, the *Completion* procedure (step 5) corresponds to IC life cycle phases 4 and 5 (Packaging and Composite Product Integration), whereas *Installation* is the IC personalization life cycle phase 6.1.

55 *Application Note 5:* The IC personalization phase should not be confused with the electronic document personalization, which takes place only in the next life cycle phase of the TOE.

56 Some production steps, e.g., Step 4 may also take place after the TOE is finished, but before the TOE is delivered to the Personalization Agent, i.e., in step 6.2 of this phase. In this case TOE's manufacturing is a usage of the TOE in a secure environment covered by the guidance documentation and is therefore subject of evaluation.

57 The security environment for the TOE and the ST of the underlying platform match, the IC life cycle phases up to 6 are covered by a controlled environment as required in [HWCR, p. 41]. In IC life cycle phase 7 no restrictions apply.

58 **TOE delivery takes place after life cycle phase 2 according to [MREDPP]. This corresponds to the end of step 6.1 according to [MREDPP]. The TOE is delivered as a chip with a completed Operating System and a ready to personalization object system.**

Life cycle phase 3 "Personalization of the Electronic Document"

59 *Step 6.2*: The personalization of the electronic document includes

1. the survey of the electronic document holder's biographical data,
2. the enrollment of the electronic document holder's biometric reference data, such as a digitized portrait or other biometric reference data,
3. printing the visual readable data onto the physical part of the electronic document, and
4. configuration of the TSF, if necessary.

60 Configuration of the TSF is performed by the *Personalization Agent* and includes, but is not limited to, the creation of the digitized version of the textual, printed data, the digitized version of e.g. a portrait, or a cryptographic signature of a cryptographic hash of the data that are stored on the chip. The personalized electronic document, if required together with appropriate guidance for TOE use, is handed over to the electronic document holder for operational use.

61 *Application Note 6*: TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies [CC]. Here TSF data include, but are not limited to, the personalization agent's key and authentication data.

62 From a hardware point of view, this cycle phase is already an operational use of the composite product and not a personalization of the hardware. The hardware's "Personalization" (cf. [HWST]) ends with the *Installation* of the TOE (installation of the object system).

63 The Personalization with User Data, e.g. cardholder identification data, may be separated from the personalization of the TOE as Qualified Signature Creation Device, e.g. the generation of a signature key.

64 The Personalization as a personalized SSCD includes the SVD certification for the intended user according to [eIDAS] and the delivery to the legitimate user.

This life cycle phase corresponds to the first step of Phase 7 of [ICPP].

Life cycle phase 4 “Operational Use”

65 *Step 7*: The chip of the TOE is used by the electronic document and terminals that Verify the chip’s data during the phase operational use. The user data can be read and modified according to the security policy of the issuer.

1.3.5 Non-TOE hardware/software/firmware

66 In order to be powered up and to communicate with the ‘external world’ the TOE needs a terminal (card reader) supporting the contactless communication according to [ISO14443].

67 According to [EACTR] the TOE is able to recognize the following terminal types:

- *PACE terminal:* A PACE terminal is a basic inspection system. It performs the standard inspection procedure, i.e. PACE followed by Passive Authentication. Afterwards user data are read by the terminal. A PACE terminal is allowed to read only common user data.

  EAC1 terminal (if the TOE contains an ICAO-conformant ePass application): An EAC1 terminal is an extended inspection system according to [EACTR-1]. It performs the advanced inspection procedure ([EACTR-1]) using EAC1, i.e. PACE, then Chip Authentication 1 followed by Passive Authentication, and finally Terminal Authentication 1. Afterwards user data are read by the terminal. An EAC1 terminal is allowed to read both EAC1 protected data, and common user data.
- *EAC2 terminal (if the TOE contains an eID application).* An EAC2 terminal is an extended inspection system performing the general authentication procedure according to [EACTR-2] using EAC2, i.e. PACE, then Terminal Authentication 2 followed by Passive Authentication, and finally Chip Authentication 2. Depending on its authorization level, an EAC2 terminal is allowed to read out some or all EAC2 protected sensitive user data, and common user data.

68 In general, the authorization level of a terminal is determined by the effective terminal authorization. The authorization is calculated from the certificate chain presented by the terminal to the TOE. It is based on the Certificate Holder Authorization Template (CHAT). A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the electronic document presenter’s restricting input at the terminal. The final CHAT reflects the effective authorization level and is then sent to the TOE [EACTR-3]. For the access rights, cf. also the SFR component FDP_ACF.1/TRM in chap. 6.1.5 (para 445).

69 All necessary certificates of the related public key infrastructure – Country Verifying Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Terminal Certificates – must be available in the card verifiable format defined in [EACTR-3].

70 The term *terminal* within this ST usually refers to any kind of terminal, if not explicitly mentioned otherwise. Which of the above terminals are related to what application and which data group is accessible by these terminals was given already in chapter 1.3.3.

71 Others than above listed terminals are out of scope of this ST. In particular, terminals using Basic Access Control (BAC) are not supported by the TOE.

72 There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

1.3.6 TOE Boundaries

1.3.6.1 TOE Physical Boundaries

73 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.

74 The chip is embedded in a module, which provides the capability for standardized connection to systems separate from the chip through TOE's interfaces in accordance with ISO standards.

75 The physical constituent of the TOE is the initialized chip with an operating system in ROM and EEPROM and an installed object system in a dedicated configuration.

76 After the *Installation* of the object system, the TOE can be personalized for the end-usage phase for the document holder as an electronic document.

1.3.6.2 TOE Logical Boundaries

77 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.

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

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

1.3.7 Conformance to eIDAS

80 In [eIDAS] the European Parliament and the Council of the European Union has codified the conceptional requirements for qualified electronic signature devices used in the European Union. In the supporting Implementing Decision is stated that an electronic signature device according to eIDAS must be certified using the standards [CC] and [SSCDPP]. As shown in this ST the TOE fulfills these standards and is therefore compliant to signature creation devices according to points (a) of Article 30(3) or 39(2) of the Regulation for qualified electronic signature or seal creation devices.

2 Conformance Claim

2.1 CC Conformance Claims

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

Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

as follows:

Part 2 extended, Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017, [CC] has to be taken into account.

2.2 PP Claims

82 This ST claims *strict* conformance to

- base Common Criteria Protection Profile 'Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use', BSI-CC-PP-0087-V2-2016-MA-01, [MREDPP], and
- its Common Criteria Protection Profile Module ‘Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates)’, BSI-CC-PP-0090-2016, [MREDONPP].

83 This implies that this ST claims also *strict* conformance to

- Common Criteria Protection Profile ‘Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP)’, BSI-CC-PP-0056-V2-2012-MA-02, [EAC1PP]
- Common Criteria Protection Profile ‘Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2_PP)’, BSI-CC-PP-0086-2015, [EAC2PP]

84 Since these PPs claim strict conformance to [PACEPP], this ST implicitly also claims *strict* conformance to

- Common Criteria Protection Profile ‘Machine Readable Travel Document using Standard Inspection Procedure with PACE’, BSI-CC-PP-0068-V2-2011-MA-01, [PACEPP].

85 However, since [EAC1PP] and [EAC2PP] already claim strict conformance to [PACEPP], this implicit conformance claim is formally mostly ignored within this ST for the sake of presentation; but if necessary to yield a better overview however, references to this Protection Profile are given or the relation with this PP is explained.

86 This ST claims also strict conformance to

- Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation, EN 419211-2:2013, BSI-CC-PP-0059-2009-MA-02 ([SSCDPP])

87 *Application Note 7:* The conformance claim to SSCDPP 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], this ST specifies authentication and communication protocol (PACE) that have to be used for the eSign application of the TOE over the contact-less interface. This contributes to secure Signature Verification Data (SVD) export, Data To Be Signed (DTBS) import, and Verification Authentication Data (VAD) import functionality.

2.3 Package Claims

88 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 6+.

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

2.4 Conformance Claim Rationale

90 The TOE type is a chip consistent with the TOE type of the claimed PP ([MREDPP]).

91 The PP [MREDPP] conforms to the PPs [EAC1PP], [EAC2PP] and [SSCDPP].This implies for this ST:

1. The TOE type of this ST is the same as the TOE type of the claimed PPs: The Target of Evaluation (TOE) is an electronic document implemented as a smart card programmed according to [EACTR], and additionally representing for the eSign application a combination of hardware and software configured to securely create, use and manage signature-creation data.
2. The security problem definition (SPD) of this ST contains the SPD of the claimed PPs. The SPD contains all threats, organizational security policies and assumptions of the claimed PPs.
3. The security objectives for the TOE in this ST include all the security objectives for the TOE of the claimed PPs.
4. The security objectives for the operational environment in this ST include all security objectives for the operational environment of the claimed PPs.
5. The SFRs specified in this ST include all security functional requirements (SFRs) specified in the claimed PPs. There are three refined SFRs within this ST:
   - The SFR FIA_UAU.1/SSCDPP is redefined from [SSCDPP] by additional assignments, this does not violate strict conformance to [SSCDPP].
   - Multiple iterations of FDP_ACF.1 and FMT_SMR.1 exist from imported PPs to define the access control SFPs and security roles for (common) user data, EAC1-

5 In this ST the backslash provides a line break for CC conformant identifiers. It should not be considered as part of the identifier. Identifiers containing natural words are hyphenated as usual.

protected user data, and EAC2-protected user data. These access control SFPs and security roles are unified to FDP_ACF.1/TRM and FMT_SMR.1

6. The SARs specified in this ST are the same as specified in the claimed PPs or extend them.

3 Security Problem Definition

3.1 Assets and External Entities

92 The primary assets are User Data to be protected by the COS as long as they are in scope of the TOE and the security services provided by the TOE (please refer to the Glossary for a definition of terms used, but not defined here).

Asset	Definition
Authenticity of the Electronic Document's Chip	The authenticity of the electronic document's chip personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document. Generic Security Property: Authenticity This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP].
Electronic Document Tracing Data	Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered. Generic Security Property: Unavailability This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP]. Note that unavailability here is required for anonymity of the electronic document holder.
Sensitive User Data	User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC1, EAC2, or both. Generic Security Properties: Confidentiality, Integrity, Authenticity
User Data stored on the TOE	All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be read out, used or modified either by a PACE terminal, or, in the case of sensitive data, by an EAC1 terminal or an EAC2 terminal with appropriate authorization level. Generic Security Properties: Confidentiality, Integrity, Authenticity This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. This asset also includes "SVD" (Integrity and Authenticity only), "SCD" of [SSCDPP].
User Data transferred between the TOE and the Terminal	All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals. Generic Security Properties: Confidentiality, Integrity, Authenticity This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. As for confidentiality, note that even though not each data element being transferred represents a secret, [EACTR-1], [EACTR-2] resp. require confidentiality of all transferred data by secure messaging in encrypt-then-authenticate mode. This asset also includes "DTBS" of [SSCDPP].

Table 1: Primary assets

93 In order to achieve a sufficient protection of the primary assets listed above, the following secondary assets are also protected by the TOE. The secondary assets represent TSF and TSF data in the sense of CC.

Asset	Definition
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. Generic Security Property: Availability
Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. Generic Security Property: Availability

Asset	Definition
Electronic Document Communication Establishment Authorization Data	Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE, and are not send to it.Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy. Generic Security Properties: Confidentiality, Integrity
Secret Electronic Document Holder Authentication Data	Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (PACE passwords). Generic Security Properties: Confidentiality, Integrity
TOE internal Non-Secret Cryptographic Material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality. Generic Security Properties: Integrity, Authenticity
TOE internal Secret Cryptographic Keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. Generic Security Properties: Confidentiality, Integrity
Secret Cryptographic Update Keys	All cryptographic key material related to the update mechanism; i.e. cryptographic material that is used to establish a secure communication channel with the update terminal, to authenticate an update terminal, to decrypt and verify the authenticity of an update package, and for other update-related cryptographic operations. Generic Security Properties: Authenticity, Confidentiality, Integrity
Meta-Data	Data that contains information about the update, e.g. version information, checksums, information w.r.t. applicability to specific product versions and platforms, etc. All Meta-Data is encrypted, any information about the update is transmitted over a secure channel between the TOE and the Update Terminal. Generic Security Properties: Authenticity, Confidentiality, Integrity
Update Data	Unencrypted data that is used to update the TOE software, e.g. data to be used to authenticate an Update Terminal. Generic Security Properties: Authenticity, Integrity
Update Log Data	Log records that store information about previously applied updates and failed update attempts. Generic Security Properties: Authenticity, Integrity
Update Package	Encrypted update data, appended with optional unencrypted meta-data, and signed. Generic Security Properties: Authenticity, Confidentiality, Integrity
Update Package Verification Status	Security attribute indicating whether the supplied update was successfully verified (and where hence its authenticity and integrity can be assumed) or not, and whether an attempt to verify was made or not. Allowed values are NOT VERIFIED, SUCCESSFULLY VERIFIED and VERIFICATION FAILED. Generic Security Properties: Authenticity, Integrity
Version Information	Version information that uniquely identify the version of the TOE software currently installed on the TOE. Generic Security Properties: Confidentiality, Integrity

Table 2: Secondary assets

94 The protection profile [MREDPP] considers the following external entities and subjects:

External entity	Definition
Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess at most high attack potential. Note that the attacker might capture any subject role recognized by the TOE.
Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues

External entity	Definition
	a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO9303].
Country Verifying Certification Authority (CVCA)	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC1 terminals, EAC2 terminals respectively, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates.
Document Signer (DS)	An organization enforcing the policy of the CSCA. A DS signs the Document Security Object that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificate , see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.
Document Verifier (DV)	An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see [EACTR-3].
Electronic Document Holder	A person the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic electronic document. This subject includes “Signatory” as defined [SSCDPP].
Electronic Document Presenter	A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker. Moreover, this subject includes “user” as defined in [SSCDPP].
Manufacturer	Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer. The manufacturer may act as Completion and Installation Agent.
PACE Terminal	A technical system verifying correspondence between the password stored in the electronic document and the related value presented to the terminal by the electronic document presenter. A PACE terminal implements the terminal part of the PACE protocol and authenticates itself to the electronic document using a shared password (CAN, PIN, PUK or MRZ). A PACE terminal is not allowed reading sensitive user data.
Personalization Agent	vAn organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic document (optical personalization) and storing them within the electronic document’s chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable [ICAO9303], [EACTR-3]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer. This subject includes “Administrator” as defined in [SSCDPP].
EAC1 Terminal / EAC2 Terminal	A terminal that has successfully passed the Terminal Authentication protocol (TA) version 1 is an EAC1 terminal, while an EAC2 terminal needs to have successfully passed TA version 2. Both are authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role terminal is the default role for any terminal being recognized by the TOE as neither being authenticated as a PACE terminal nor an EAC1 terminal nor an EAC2 terminal.

Table 3: External Entities[6]

6 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]). From this point of view, the TOE itself perceives only ‘subjects’ and, for them, 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.

3.2 Threats

95 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 stored in or protected by the TOE and the method of TOE's use in the operational environment.

96 The threats, which are defined in the Protection Profile [ICPP] are already covered by claimed Protection Profiles and are therefore not considered in this ST.

97 The following threats are specified in the Protection Profile [MREDPP].

T.InconsistentSec Inconsistency of security measures

98 An attacker gains read or write access to user data or TOE data without being allowed to, due to an ambiguous/unintended configuration of the TOE's internal access conditions of user or TSF data. This may lead to a forged electronic document or misuse of user data.

99 Threat agent has high attack potential, and may be in possession of one or more legitimate electronic documents.

Asset: authenticity, integrity and confidentiality of user data stored on the TOE

T.Interfere Interference of security protocols

100 An attacker uses an unintended interference of implemented security protocols to gain access to user data.

101 Threat agent has high attack potential, and may be in possession of one or more legitimate electronic documents.

102 Asset: authenticity, integrity and confidentiality of user data stored on the TOE

T.AdvancedTracing Advanced Tracing and Group Key Compromise

103 The attacker compromises a group key or is able to trace and identify the electronic document holder by key material that is used to guarantee the authenticity of the document. Tracing is often (e.g. in the case of Chip Authentication 2) avoided by using one key for a group of electronic documents. If the group is large enough, individual tracing is no longer possible. If an attacker compromises such a group key however, authenticity of all of the electronic documents within the group can be guaranteed. On the other hand, if chip individual keys are used to ensure the authenticity of the document, only a single document is affected by a key compromise. However then, the (public) chip-individual keys can be misused for tracing the document and its holder.

104 Threat agent: having high attack potential, being in the possession of one or more legitimate electronic documents

105 Asset: authenticity, integrity, and confidentiality of user data stored on the TOE

106 The following threats are specified in the Protection Profile Module [MREDONPP].

T.FaTSF Faulty TSF

107 Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF, for example due to:

- software issues that were not detected, not exploitable, or deemed unable to being exploitable at the time of certification, but due to unforeseen advances in technology became a security risk during operational use of the TOE, or
- cryptographic mechanisms that were deemed secure at the time of certification, but due to unforeseen advances in the field of cryptography became a security risk during operational use of the TOE.

108 Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

109 Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

T.UaU Unauthorized Update

110 Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF by misuse of the update functionality. This threat contains two main aspects:

- the unauthorized installation, which may lead to the use of untimely, outdated or revoked updates,
- the installation of updates that are not authorized and authentic.

111 Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

112 Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

113 The following threats are included from [EAC1PP]. They concern EAC1-protected data.

T.Counterfeit Counterfeit of travel document chip data

114 An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document.

115 The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

116 Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

117 Asset: authenticity of user data stored on the TOE

T.Read_Sensitive_Data DataRead the sensitive biometric reference data

118 Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.

119 The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [8]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

120 Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document

121 Asset: confidentiality of logical travel document sensitive user data (i.e. biometric reference)

122 The following threats are included from [EAC2PP]. They concern EAC2-protected data.

T.Counterfeit/EAC2 Counterfeit of electronic document chip data

123 Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for authentication of a electronic document presenter by possession of an electronic document. The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document.

124 Threat agent: having high attack potential, being in possession of one or more legitimate ID-Cards.

125 Asset: authenticity of user data stored on the TOE

T.Sensitive_Data Unauthorized access to sensitive user data

126 Adverse action: An attacker tries to gain access to sensitive user data through the communication interface of the electronic document's chip. The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack (sensitive data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

127 Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate electronic document

128 Asset: confidentiality of sensitive user data stored on the electronic document

129 The following threats are included from [PACEPP]. Both [EAC1PP] and [EAC2PP] claim [PACEPP], and thus include the threats formulated in [PACEPP]. We list each threat only once here.

T.Abuse-Func Abuse of Functionality

130 An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclosure the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the Passport holder.

131 *Application Note 8:* 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.Eavesdropping Eavesdropping on the communication between the TOE and the PACE terminal

132 An attacker is listening to the communication between the Travel document and the PACE terminal (PCT) in order to gain the user data transferred between the TOE and the service provider (inspecting authority) connected.

133 *Application Note 9:* A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP. When using EIS-AIP-BAC, this threat might be averted only with respect to a selected data groups (DG3, DG4) within the ePass application, but it is out of the scope of the current PP; see also the Application Note 2 above.

T.Forgery Forgery of Data

134 An attacker fraudulently alters the User Data or/and TSF-data stored on the ePass or/and exchanged between the TOE and the service provider (inspecting authority) connected in order to outsmart the authenticated terminal (PCT) by means of changed ePass holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the service provider (represented by the terminal connected) perceives these modified data as authentic one.

T.Information_Leakage Information Leakage from travel document

135 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 travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

136 *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 Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover, the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Malfunction Malfunction due to Environmental Stress

137 An attacker may cause a malfunction the ePass'es hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE's 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 ePass outside the normal operating conditions, exploiting errors in the ePass'es Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

138 *Application Note 11:* 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 TOE's internals.

T.Phys-Tamper Physical Tampering

139 An attacker may perform physical probing of the ePass in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the ePass in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the ePass.

140 *Application Note 12:* 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 ePass) 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 a direct interaction with the ePass's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, 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.Skimming Skimming ePass / Capturing Card-Terminal Communication

141 An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the service provider (inspecting authority) 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) in advance.

142 *Application Note 13:* A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP. When using EIS-AIP-BAC, this threat might be averted only with respect to a selected data groups (DG3, DG4) within the ePass application, but it is out of the scope of the corresponding PP.

143 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]). 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.

144 *Application Note 14*: This threat also covers the item T.Read_Sensitive_Data in the ICAO-EAC PP [ICAO9303]: sensitive biometric reference data stored on the travel document

are part of the asset user data stored on the TOE. Knowledge of the Document Basic Access Keys is here not applicable, because the TOE does not cover the BAC protocol and, therefore, the Document Basic Access Keys are not existent for the TOE.

145 *Application Note 15:* MRZ is printed and CAN is printed or stuck on the Travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Card-Holder.

T.Tracing Tracing travel document

146 An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE. The attacker cannot read and does not know the correct values of shared passwords (CAN, MRZ) in advance.

147 *Application Note 16:* 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 this PP, see also the Application Note 2 above.

148 *Application Note 17:* Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.

149 The following threats are included from [SSCDPP]. These items are applicable if the eSign application is operational.

T.DTBS_Forgery Forgery of the DTBS/R

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

T.Hack_Phys Physical attacks through the TOE interfaces

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

T.SCD_Derive Derive the signature-creation data

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

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

153 An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature-creation in the TOE.

T.Sig_Forgery Forgery of the digital signature

154 Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

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

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

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

156 An attacker presents a forged SVD to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

3.3 Organizational Security Policies

157 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 (see CC part 1, sec. 3.2). This ST includes the OSPs from the claimed protection profiles as listed below and provides no further OSPs.

158 The following OSP is defined in [MREDPP] akin to the Protection Profile [ICPP]. It addresses the need of a policy for the document manufacturer. Please refer to [ICPP] for further descriptions and the details.

P.Lim_Block_Loader

159 The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. She limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.

160 The following OSPs are defined in the EAC1 PP [EAC1PP]:

P.Personalization **Personalization of the travel document by issuing State or Organization only**

161 The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organization only.

P.Sensitive_Data **Privacy of sensitive biometric reference data**

162 The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems, which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). 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. The travel document'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 Version 1.

163 The following OSPs are defined in the EAC2 PP [EAC2PP]:

P.EAC2_Terminal Abilities of Terminals executing EAC Version 2

164 Terminals that intent to be EAC2 terminals must implement the respective terminal part of the protocols required to execute EAC version 2 according to [TR03110-2], and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

P.RestrictedIdentity Restricted Identity and Sector's Static Key Pairs

165 If the TOE supports the Restricted Identity protocol, the electronic document issuer shall ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as defined in [EACTR-2].

P.Terminal_PKI PKI for Terminal Authentication

166 The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

167 The following OSPs are defined in the PACE PP [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP]. We list each OSP only once here.

P.Card_PKI PKI for Passive Authentication (issuing branch)

168 *Application Note 18:* The description below states the responsibilities of 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.

169 1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall make the CSCA Certificate (C_{CSCA}) and the Document Signer Certificates (C_{DS}) available to the CVCAs under agreement (who shall finally distribute them to their terminals).

170 2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer.

171 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 and (iv) securely use the Document Signer

P.Manufact Manufacturing of the travel document's chip

172 The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

P.Pre-Operational Pre-operational handling of the travel document

173 1. The travel document Issuer issues the travel document and approves using the terminals complying with all applicable laws and regulations.

174 2. The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.

175 3. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel document in their manufacturing and issuing life phases, i.e. before they are in the operational phase.

176 4. If the travel document Issuer authorizes a Personalization Agent to personalize the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the travel document Issuer's policy.

P.Terminal Abilities and trustworthiness of terminals

177 The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

178 1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO9303].

179 2. They shall implement the terminal parts of the PACE protocol [ICAOSAC], of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).

180 3. The related terminals need not to use any own credentials.

181 4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document [6]).

182 5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP ().

P.Trustworthy_PKI Trustworthiness of PKI

183 The CSCA shall ensure that it issues its certificates exclusively to the rightful organizations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects having to be stored on the travel document.

184 The following OSPs are defined in the SSCD PP [SSCDPP]. They are applicable, if the eSign application is included.

P.CSP_QCert Qualified certificate

185 The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. [eIDAS, Article 3 clause 15 and Annex I]) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign Qualified electronic signatures

186 The signatory uses a signature-creation system to sign data with an advanced electronic signature according to [eIDAS], which is a qualified electronic signature if it is based on a valid qualified certificate. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sig_Non-Repud Non-repudiation of signatures

187 The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in his un-revoked certificate.

P.Sigy_SSCD SSCD TOE as secure signature-creation device

188 The TOE meets the requirements for an SSCD laid down in the eIDAS Regulation and its Implenenting Acts []eIDAS]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

189 The following OSPs are defined in the PP Module [MREDONPP]:

P.Code_Confidentiality

190 Update code packages that are created by the TOE software developer or document manufacturer are kept confidential, are encrypted after development at the site of the electronic document manufacturer, and are delivered to the TOE in encrypted form.

P.Secure_Environment

191 Update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. Authorized staff oversees the complete update procedure.

P.Eligible_Terminals_Only

192 Update terminals (i.e. terminals with appropriate certificates that are able to install updates) are handed only to those entities where P.Secure_Environment is enforced. In case of a security incident, these update terminals are functionally disabled (through organizational and/or cryptographic means by e.g. withdrawing certificates).

3.4 Assumptions

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

194 The assumptions A.Process-Sec-IC, A.Plat-Appl and A.Resp-Appl defined in the Protection Profile [ICPP] are not relevant for this ST.

195 The following assumptions are included from [EAC1PP]. They concern EAC1-protected data.

A.Auth_PKI PKI for Inspection Systems

196 The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

A.Insp_Sys Inspection Systems for global interoperability

197 The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAOSAC] and/or BAC [BACPP]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

198 [EAC2PP] only includes the assumption from [PACEPP] (see below) and defines no other assumption.

199 The following assumptions are included from PACE PP [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP]. We list each OSP only once here.

A.Passive_Auth PKI for Passive Authentication

200 The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document

Security Object contains only the hash values of genuine user data according to [ICAO9303].

201 The following assumptions are included from SSCD PP [SSCDPP]. They are applicable, if the eSign application is included.

A.CGA Trustworthy certificate generation application

202 The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA Trustworthy signature creation application

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

204 No additional assumptions are made by the PP Module [MREDONPP].

4 Security Objectives

205 This chapter describes the security objectives for the TOE and for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development, and production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

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

207 The following Security Objectives for the TOE are defined in the Protection Profile [ICPP] for the Loader and are relevant for the electronic document manufacturing process ([MREDPP]). A loader is a part of the chip operating system that allows to load data, i.e. the object system containing (sensitive) user data, TSF data etc. into the Flash or EEPROM memory after delivery of the smart card to the document manufacturer.

OT.Cap_Avail_Loader Availability of the Loader Functionality

208 The TSF provides limited capability of the Loader functionality of the TOE embedded software and irreversible termination of the Loader in order to protect user data from disclosure and manipulation.

209 The following objective is defined in ([MREDPP]) and concerns the consistency of the access control mechanisms.

OT.Non_Interfere No interference of Access Control Mechanisms

210 The various implemented access control mechanisms must be consistent. Their implementation must not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

OT.CA3 Protection against advanced tracing techniques using Chip Authentication 3

211 The TOE provides the Chip Authentication 3 protocol. Chip Authentication 3 provides a message-deniable strong explicit authentication of the electronic document, pseudonymity of the electronic document without the need to use the same keys on several chips, and the possibility of whitelisting electronic documents, even in the case of a group key compromise. (cf. [EACTR-2-v2.20]).

212 The following objectives are included from [EAC1PP]. They concern EAC1-protected data. For the remaining security objectives see the next sections.

OT.Chip_Auth_Proof Proof of the travel document's chip authenticity

213 The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Chip Authentication Version 1 as defined in [5]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

214 *Application Note 19:* The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

215 The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Chip_Auth_Proof_PACE_CAM Proof of the electronic document's chip authenticity(Refinement of OT.Chip_Auth_Proof)

216 The TOE must support the **Terminals** ~~Inspection Systems~~ to verify the identity and authenticity of the ~~travel~~ **electronic** document's chip as issued by the identified issuing State or Organization by means of the ~~Chip Authentication Version 1 as defined in [EACTR-1]~~ **PACE-Chip Authentication Mapping (PACE-CAM) as defined in [ICAO9303]**. The authenticity proof provided by travel electronic document's chip shall be protected against attacks with high attack potential.

217 *Application Note 20:* PACE-CAM enables much faster authentication of the of the chip than running PACE with General Mapping (according to [TR03110-1]) followed by CA1.ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

218 The following objectives are included from [EAC2PP]. They concern EAC2-protected data. For the remaining security objectives see the next sections. Note that justifications made in the PP will not be repeated here. Please refer to the Protection Profile [EAC2PP].

OT.AC_Pers_EAC2 Personalization of the Electronic Document

219 The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access

rights. The access rights are determined by the electronic document during Terminal Authentication 2.

OT.CA2 Proof of the Electronic Document's Chip Authenticity

220 The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [EACTR-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.

OT.RI_EAC2 Support of Restricted Identity by the TOE

221 If the TOE supports pseudonymous authentication, it must use the Restricted Identity protocol as defined in [EACTR-2].

OT.Sens_Data_EAC2 Confidentiality of sensitive User Data

222 The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE.

223 The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

224 The following objectives are included from PACE PP [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

OT.AC_Pers Access Control for Personalization of logical MRTD

225 The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO9303] and the TSF data can be written by authorized Personalization Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.

226 *Application Note 21:* The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalization.

OT.Data_Authenticity Authenticity of Data

227 The TOE must ensure authenticity of the User Data and the TSF-data31 stored on it by enabling verification of their authenticity at the terminal-side32.The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality Confidentiality of Data

228 The TOE must ensure confidentiality of the User Data and the TSF-data34 by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Integrity Integrity of Data

229 The TOE must ensure integrity of the User Data and the TSF-data30 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 during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Identification Identification of the TOE

230 The TOE must provide means to store Initialization[7] 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 cycle phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

OT.Prot_Abuse-Func Protection against Abuse of Functionality

231 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.

OT.Prot_Inf_Leak Protection against Information Leakage

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

- 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.

233 *Application Note 22:* 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_Malfunction Protection against Malfunctions

234 The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have 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.

[7] amongst other, IC Identification data

OT.Prot_Phys-Tamper Protection against Physical Tampering

235 The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document'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.

OT.Tracing Tracing travel document

236 The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

237 *Application Note 23:* Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity) cannot be achieved by the current TOE.

238 The following objectives are included from SSCD PP [SSCDPP]. They are applicable, if the eSign application is included.

OT.DTBS_Integrity_TOE DTBS/R integrity inside the TOE

239 The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

OT.EMSEC_Design Provide physical emanations security

240 The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security Lifecycle security

241 The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

242 *Application Note 24:* The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD_Secrecy Secrecy of the signature creation data

243 The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

244 *Application Note 25:* The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

OT.SCD_SVD_Corresp Correspondence between SVD and SCD

245 The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.SCD_Unique Uniqueness of the signature creation data

246 The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD/SVD_Auth_Gen Authorized SCD/SVD generation

247 The TOE shall provide security features to ensure that authorized users only may invoke the generation of the SCD and the SVD.

OT.Sig_Secure Cryptographic security of the electronic signature

248 The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF Signature creation function for the legitimate signatory only

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

OT.Tamper_ID Tamper detection

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

OT.Tamper_Resistance Tamper resistance

251 The TOE shall prevent or resist physical tampering with specified system devices and components.

252 A careful analysis reveals that the formally listed here objectives OT.SCD_Secrecy, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, and OT.Tamper_Resistance are actually fully or partly covered by security objectives included from the [PACEPP].

253 The following objectives are included from PP Module [MREDONPP].

OT.Update_MechanismTOE Update Mechanism

254 The TSF provides a mechanism to install code-signed updates of the TOE software by authorized staff during operational use.

OT.Enc_Sign_Update Encrypted-then-signed Update Packages

255 The TOE only installs update packages that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates.

OT.Update_Terminal_Auth Updates only by authenticated Update Terminals

256 The TOE allows only authenticated update terminals to upload an update package to the TOE and to initiate the update procedure. The TOE uses a dedicated cryptographic method described in the TCOS Admin Guidance [TCOSGD] to authenticate an update terminal.

OT.Attack_Detection Detection of Attacks on the TOE using the Update Mechanism

257 The TOE has logging capabilities that track installed updates and failed update attempts. It also limits the amount of faulty (signature verification or decryption fails) update attempts. It allows dedicated terminals to read out the update logs.

OT.Key_Secrecy Key Secrecy of Cryptographic Update Keys

258 The TOE keeps the cryptographic update keys secret, and is designed such that emissions from the TOE do not allow to read out or gain full or partial information about the keys.

4.2 Security Objectives for the Operational Environment

259 These objectives for the environment are extended to the electronic document manufacturing process by the following objective defined in ([MREDPP]).

OE.Lim_Block_Loader

260 The manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

261 *Justification:* This security objective directly addresses the threat OT.Non_Interfere. This threat concerns the potential interference of different access control mechanisms, which could occur as a result of combining different applications on a smartcard. Such combination does not occur in one of the claimed PPs. Hence, this security objective for the environment does

- neither mitigate a threat of one of the claimed PPs that was addressed by security objectives of that PP,
- nor does it fulfill any organizational security policy of one of the claimed PPs that was meant to be addressed by security objectives of the TOE of that PP.

262 The following objectives are included from [EAC1PP]. They concern EAC1-protected data. For the remaining security objectives see the next sections. Note that justifications made in the PP will not be repeated here. Please refer to the Protection Profile [EAC1PP].

OE.Auth_Key_Travel_Document Travel document Authentication Key

263 The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify

the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

264 The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.Exam_Travel_Document Examination of the physical part of the travel document

265 The inspection system of the receiving State or Organization must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [ICAO9303] and/or the Basic Access Control [BACPP]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

266 The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

OE.Prot_Logical_Travel_Document Protection of data from the logical travel document

267 The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

268 The following objectives are included from [EAC2PP]. They concern EAC2-protected data. For the remaining security objectives see the next sections. Note that justifications made in the PP will not be repeated here. Please refer to the Protection Profile [EAC2PP].

OE.Chip_Auth_Key Key Pairs needed for Chip Authentication and Restricted Identification

269 The electronic document issuer has to ensure that the electronic document's chip authentication key pair and the Restricted Identification key pair are generated securely, that the private keys of these key pairs are stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [EACTR-2] to check the authenticity of the electronic document's chip.

OE.RestrictedIdentity Restricted Identity and Sector's Static Key Pairs

270 If the TOE supports pseudonymous identification and thus implements the Restricted Identity protocol, the electronic document issuer has to ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as required according to [EACTR-2].

OE.Terminal_Authentication Key pairs needed for Terminal Authentication

271 The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

272 The following objectives are included from PACE PP [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

OE.Legislative_Compliance Issuing of the travel document

273 The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

OE.Passive_Auth_Sign Authentication of travel document by Signature

274 The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically 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) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.

275 A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically 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 Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO9303. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO9303]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalization Personalization of travel document

276 The travel document Issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Travel document (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [ICAO9303], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO9303] (in the role of a DS).

OE.Terminal Terminal operating

277 The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO9303].
2. The related terminals implement the terminal parts of the PACE protocol [ICAOSAC], of the Passive Authentication [ICAOSAC] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).
3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO9303]).
5. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

278 *Application Note 26:* OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [BACPP].

OE.Travel_Document_Holder Travel document holder Obligations

279 The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

280 The following objectives are included from SSCD PP [SSCDPP]. They are applicable, if the eSign application is included.

OE.CGA_QCert Generation of qualified certificates

281 The CGA generates a qualified certificate that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP.

282 The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in a SSCD.

OE.DTBS_Intend SCA sends data intended to be signed

283 The Signatory uses trustworthy SCA that

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

OE.DTBS_Protect SCA protects the data intended to be signed

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

OE.HID_VAD Protection of the VAD

285 If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

OE.Signatory Security obligation of the Signatory

286 The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The Signatory keeps his or her VAD confidential.

OE.SSCD_Prov_Service Authentic SSCD provided by SSCD Provisioning Service

287 The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalizes and delivers the TOE as SSCD to the signatory.

OE.SVD_Auth Authenticity of the SVD

288 The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

289 The following objectives are included from PP Module [MREDONPP].

OE.Code_Confidentiality

290 The operational environment must ensure that the TOE software developer or document manufacturer keeps update code packages confidential, encrypts them after development at the site of the developer/manufacturer, and delivers them to the TOE in encrypted form.

291 This objective is applicable in the Development and Production Environment, whereas the following are related to the Operational Environment.

OE.Secure_Environment

292 The operational environment must ensure that update terminals are placed in a secure environment that prevents unauthorized physical access and are operated by authorized staff only. The operational environment must also ensure through e.g. organizational policies and procedures, that authorized staff oversees the complete update procedure.

OE.Eligible_Terminals_Only

293 The operational environment must also ensure by, e.g. organizational procedures, supported by cryptographic means, that only those entities that have policies in place that guarantee OE.Secure_Environment, are supplied with update terminals. Moreover, the operational environment guarantees that update terminals can be functionally deactivated if these policies are no longer in place or not enforced at the entities. This is implemented by the issuance of certificates for update terminals in a corresponding public key infrastructure.

294 *Justification:* Each of these security objectives on the environment directly addresses one of the organizational security policies P.Code_Confidentiality, P.Secure_Environment, and P.Eligible_Terminals_Only. Hence, these security objectives for the environment do

- neither mitigate a threat of the base PP that was addressed by security objectives of the base PP,
- nor do they fulfill any organizational security policy of the base PP that was meant to be addressed by security objectives of the TOE of the base PP.

295 Note in particular that OE.Eligible_Terminals_Only requires a general issuance and revocation mechanism or update terminals and leaves the specific implementation open, whereas OE.Terminal_Authentication of the base PP specifically addresses certificates for EAC2 terminals.

4.3 Security Objective Rationale

296 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.

	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification	O.RND	OT.Cap_Avail_Loader	OT.Non_Interfere	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE_CAM	OT.AC_Pers_EAC2	OT.CA2	OT.CA3	OT.RI_EAC2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance	OT.Update_Mechanism	OT.Enc_Sig_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy
T.Leak-Inherent	x																																												
T.Phys-Probing		x																																											
T.Malfunction			x																																										
T.Phys-Manipulation				x																																									
T.Leak-Forced					x																																								
T.Abuse-Func						x																																							
T.RND								x																																				
T.InconsistentSec									x	x		x		x		x		x	x	x	x	x																						
T.Interfere										x																																			
T.Counterfeit											x		x			x																												
T.Read_Sensitive_Data												x																																
T.Counterfeit/EAC2															x																													
T.AdvancedTracing																x																												
T.Sensitive_Data																		x																										
T.Abuse-Func																								x																				
T.Eavesdropping																					x																						
T.Forgery																			x	x	x	x		x			x																
T.Information_Leakage																									x																			
T.Malfunction																										x																		
T.Phys-Tamper																											x																	
T.Skimming																				x	x	x																						
T.Tracing																												x																
T.DTBS_Forgery																													x															
T.Hack_Phys																															x													
T.SCD_Derive																																			x	x								
T.SCD_Divulg																															x													

	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification	O.RND	OT.Cap_Avail_Loader	OT.Non_Interfere	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE_CAM	OT.AC_Pers_EAC2	OT.CA2	OT.CA3	OT.RI_EAC2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance	OT.Update_Mechanism	OT.Enc_Sig_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy
T.Sig_Forgery																																	x		x									
T.SigF_Misuse																												x		x						x							
T.SVD_Forgery																																x											
T.FaTSF																																							x			x	x
T.UaU																																								x	x		
P.Personalization							x															x																					
P.Sensitive_Data												x																															
P.RestrictedIdentity																	x																										
P.Manufact							x																																			
P.Pre-Operational							x												x																							
P.CSP_QCert																														x		x										
P.QSign																																				x	x					
P.Sig_Non-Repud																												x	x	x	x	x	x		x	x	x	x				
P.Sigy_SSCDPP																												x	x	x	x		x		x	x		x				
P.Lim_Block_Loader									x	x																																
P.Process-TOE							x																																			

Table 4:Security Objective Rationale for the TOE

	OE.Resp-Appl	OE.Process-Sec-IC	OE.Lim_Block_Loader	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Ext_Insp_Systems	OE.Ext_Insp_Systems	OE.Chip_Auth_Key	OE.RestrictedIdentity	OE.Terminal_Authentication	OE.Legislative_Compliance	OE.Passive_Auth_Sign	OE.Personalization	OE.Terminal	OE.Travel_Document_Holder	OE.CGA_QCert	OE.DTBS_Intend	OE.DTBS_Protect	OE.HID_VAD	OE.Signatory	OE.SSCD_Prov_Service	OE.SVD_Auth	OE.Code_Confidentiality	OE.Secure_Environment	OE.Eligible_Terminals_Only
T.Counterfeit				x		x																				
T.Skimming																x										
T.Tracing																x										
T.Forgery													x	x	x	x										
T.SigF_Misuse																				x						
P.Personalization														x												
P.Sensitive_Data					x		x																			
P.Pre-Operational												x		x												
P.EAC2_Terminal									x		x				x											
P.RestrictedIdentity										x																
P.Terminal_PKI											x															
P.Card_PKI													x													
P.Terminal						x									x											
P.Trustworthy_PKI													x													
P.CSP_QCert																	x									
P.QSign																	x									
P.Sig_Non-Repud																	x	x	x		x	x	x			
P.Sigy_SSCDPP																						x				
P.Lim_Block_Loader			x																							
P.Process-TOE	x																									
P.Code_Confidentiality																								x		
P.Secure_Environment																									x	

	OE.Resp-Appl	OE.Process-Sec-IC	OE.Lim_Block_Loader	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Ext_Insp_Systems	OE.Ext_Insp_Systems	OE.Chip_Auth_Key	OE.RestrictedIdentity	OE.Terminal_Authentication	OE.Legislative_Compliance	OE.Passive_Auth_Sign	OE.Personalization	OE.Terminal	OE.Travel_Document_Holder	OE.CGA_QCert	OE.DTBS_Intend	OE.DTBS_Protect	OE.HID_VAD	OE.Signatory	OE.SSCD_Prov_Service	OE.SVD_Auth	OE.Code_Confidentiality	OE.Secure_Environment	OE.Eligible_Terminals_Only
P.Eligible_Terminals_Only																										x
A.Process-Sec-IC		x																								
A.Process-Sec-SC		x																								
A.Resp-Appl	x																									
A.Auth_PKI					x			x																		
A.Insp_Sys						x																				
A.Passive_Auth						x							x													
A.CGA																	x						x			
A.SCA																		x								

Table 5:Security Objective Rationale for the Environment

For the additional threats the corresponding rationale is given in the claimed by this ST Protection Profile [MREDPP], its Module [MREDONPP] or in the claimed therein PPs. Hence, it will not be repeated here.

5 Extended Components Definition

297 This Security Target includes all extended components from the claimed PPs. This includes families FAU_SAS, FCS_RND, FMT_LIM and FPT_EMS from [PACEPP] and FIA_API from [EAC2PP].

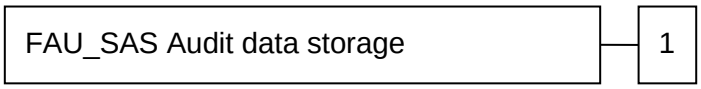
5.1 FAU_SAS Audit data storage

298 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.

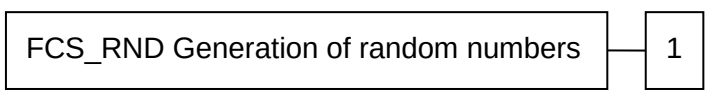
5.2 FCS_RND Generation of random numbers

299 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 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 Random number generation

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

300 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 leveling:

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, or of the TOE itself*].

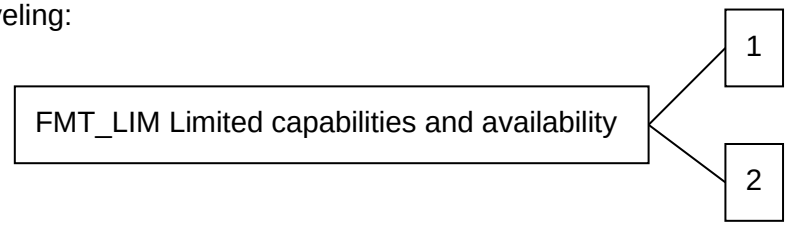
5.4 FMT_LIM Limited capabilities and availability

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

Family behavior

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 component 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 life-cycle.

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.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed and implemented 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*].

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed and implemented 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*].

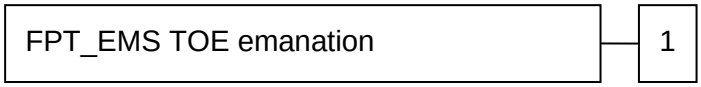
5.5 FPT_EMS TOE Emanation

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMS.1 Emanation of TSF and User data, defines limits of TOE emanation related to TSF and User data.

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No other components.

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

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

6 Security Requirements

303 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.

304 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.

305 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~~. Refinements made by the ST author appear ***slanted, bold and underlined***.

306 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*.

307 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*.

308 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.

309 In order to distinguish between SFRs defined here and SFRs that are taken over from PPs to which this PP claims strict conformance, the latter are iterated or renamed in the following way[8]:

/EAC1PP or /□□□_EAC1PP [EAC1PP],

/EAC2PP or /□□□_EAC2PP for [EAC2PP],

and /SSCDPP or /□□□_SSCDPP for [SSCDPP].

310 The SFRs related to the module PP [MREDONPP] are marked with the iteration /UPD or /UPD_□□□.

311 The SFRs related to the IC Platform are marked with the iteration /ICP.

6.1 Security Functional Requirements for the TOE

312 The statements of security requirements must be internally consistent. As several different PPs with similar SFRs are claimed, great care must be taken to ensure that these several iterated SFRs do not lead to inconsistency.

313 Both [EAC1PP] and [EAC2PP] claim strict conformance to [PACEPP]. Thus, they include all SFRs from [PACEPP]. On the other hand, due to strict conformance to [EAC1PP] and [EAC2PP], this PP includes all SFRs from [EAC1PP] and [EAC2PP]. Hence all SFRs from [PACEPP] appear in this PP twice as SFRs from [EAC1PP] and [EAC2PP], and thus SFRs

8 Here □□□ stands for the original SFR identifier.

from [PACEPP] are not listed in this PP. In other words, despite claiming strict conformance to [PACEPP], SFRs can be safely ignored during evaluation and certification as long as [EAC1PP] and [EAC2PP] are taken into account.

314 One must remember that each of these iterated SFRs mostly concerns different (groups of) user and TSF data for each protocol (i.e. PACE, EAC1 and EAC2). We distinguish three cases:

1. The SFRs apply to different data that are accessible by executing different protocols. Hence, they are completely separate. An example is FCS_CKM.1/DH_PACE from [EAC1PP] and [EAC2PP]. No remark is added in such case in the text below.
2. The SFRs are equivalent. Then we list them all for the sake of completeness. Hence, it suffices to consider only one iteration. For such SFRs, we explicitly give a remark. An example is FIA_AFL.1/PACE from [EAC1PP] and [EAC2PP].
3. The SFRs do not apply to different data or protocols but are also not completely equivalent. Then these multiple SFRs are refined in such a way, that one common component is reached that subsumes all iterations that stem from the inclusions of the claimed PPs. An example is FDP_ACF.1, which is combined here from [EAC1PP] and [EAC2PP]. Such a case is also explicitly mentioned in the text.

315 Thus, internal consistency is not violated.

6.1.1 Overview

316 To give an overview of the security functional requirements mentioned in 1.3.1 in the context of the security services offered by the TOE the security functional groups were considered, and the functional requirements described in the following sections are allocated to them. The following table provides an overview of security functional requirements in the context of the main security functionalities offered by the TOE:

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} – {FDP_ACC.1/UPD, FDP_ACF.1/UPD} Supported by: – FIA_UAU.1/EAC2_Terminal: Terminal Authentication (BIS-PACE, EIS-GAP, ATT, SGT) – {FDP_ACC.1/Signature-creation_SSCDPP, FDP_ACF.1/Signature-creation_SSCDPP} Supported by: – FIA_UAU.1/UPD – FIA_UID.1/UPD
Secure data exchange between the electronic document and the Service Provider connected	– FTP_ITC.1/CA: trusted channel for EIS-GAP, ATT, SGT – FTP_ITC.1/PACE: trusted channel for BIS-PACE – FTP_ITC.1/UPD Supported by: a) for GAP: – FCS_COP.1/PACE_ENC_EAC2PP: encryption/decryption – FCS_COP.1/PACE_MAC_EAC2PP: MAC generation/verification – FIA_API.1/CA: Chip Identification/Authentication (version 2) – FIA_UAU.1/EAC2_Terminal: Terminal Authentication (BIS-PACE, EIS-GAP, ATT, SGT) b) for AIP: – FCS_COP.1/SYM_EAC1PP: encryption/decryption – FCS_COP.1/MAC_EAC1PP: MAC generation/verification – FIA_API.1/EAC1PP: Chip Identification/Authentication (version 1)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT equiv. BIS-PACE) – FIA_UID.1/EAC2_Terminal: Terminal Identification (EIS-GAP, ATT, SGT) – FIA_UAU.1/PACE: PACE Authentication (PCT equiv. BIS-PACE) – FIA_UAU.1/EAC2_Terminal: Terminal Authentication (EIS-GAP, ATT, SGT) – FIA_API.1/CA: Chip Identification / Authentication for GAP (version 2) – FIA_API.1/EAC1PP: Chip Identification/Authentication for AIP (version 1) – FIA_UAU.4: single-use of authentication data – FIA_UAU.5: multiple authentication mechanisms – FIA_UAU.6: Re-authentication of Terminal – FIA_AFL.1/PIN_Suspending – FIA_AFL.1/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_AFL.1/UPD – FIA_UID.1/SSCDPP: Identification of electronic document holder as Signatory (eSign-PIN) – FIA_UIA.1/SSCDPP: Authentication of electronic document holder as Signatory (eSign-PIN) – FIA_AFL.1/SSCDPP: 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-GAP, ATT, SGT) – FCS_CKM.1/DH_CA: Chip Authentication – FCS_CKM.2/DH: Diffie-Hellman 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/SSCDPP Supported by: – FCS_CKM.4/SSCDPP – {FDP_ACC.1/SCD/SVD_Generation_SSCDPP, FDP_ACF.1/SCD/SVD_Generation_SSCDPP} – {FDP_ACC.1/SVD_Transfer_SSCDPP, FDP_ACF.1/SVD_Transfer_SSCDPP}
Creation of Digital Signatures by the eSign application	– FCS_COP.1/SSCDPP
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 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_SSCDPP – FDP_SDI.2/DTBS_SSCDPP Supported by: – the entire class FMT.

Table 6: Security Functional Groups vs. SFRs

317 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.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-GAP, ATT, SGT), the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the electronic document 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.
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 electronic document and the Document Security Object (SO_D) of the ePass 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 electronic document 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. [TCOSGD]).
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 electronic document.
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.
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-GAP, ATT, SGT) as result of the Chip Authentication Protocol, see, Part 2, A.4, and E.2.2, A.2.3.2.

Name	Data
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 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 [Part 1, sec. 3 and Part 2, sec. 3]. For Restricted Identification please also refer to Paragraph 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 Electronic document 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 [XXX] in order to be compliant with the European eIDAS Regulation.
Update Key	
Secret Update Key	Secret Update Key is represented by a private cryptographic key being used by the TOE to create a secure channel for the installation of packages to update TOE and User Data in the operational phase. The update mechanism is described in detail in the Guidance [TCOSGD]. Using this key, the TOE prevents the acceptance of wrong packages.

Table 7: Keys and Certificates

6.1.2 Class FAU Security Audit

318 The following SFR is imported due to claiming [PACEPP].

- FAU_SAS.1/PACEPP (equivalent to FAU_SAS.1/EAC2PP, listed here only for the sake of completeness)

319 The following SFRs are imported due to claiming [EAC1PP] and [EAC2PP] in the Protection Profile [MREDPP].

- FAU_SAS.1/EAC1PP (equivalent to FAU_SAS.1/PACEPP, listed here only for the sake of completeness)
- FAU_SAS.1/EAC2PP

320 The following SFR is imported due to claiming [MREDONPP].

- FAU_SAS.1/UPD

321 **FAU_SAS.1/EAC2PP Audit storage**

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1/EAC2PP

The TSF shall provide *the Manufacturer*[9] with the capability to store *the Initialization and Pre-Personalization Data*[10] in the audit records.

322 *Application Note 27:* The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the electronic document 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 electronic document (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.

323 **FAU_SAS.1/UPD Audit storage**

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1/UPD

The TSF shall provide **the TOE update functionality**[11] with the capability to store update log information and version history, namely the following data objects: *update package information data*[12] in the audit records.

6.1.3 Class FCS Cryptographic Support

324 The following SFRs are imported due to claiming [EAC2PP]. They concern cryptographic support for applications that contain EAC2-protected data groups.

- FCS_CKM.1/DH_PACE_EAC2PP
- FCS_COP.1/SHA_EAC2PP
- FCS_COP.1/SIG_VER_EAC2PP
- FCS_COP.1/PACE_ENC_EAC2PP
- FCS_COP.1/PACE_MAC_EAC2PP
- FCS_CKM.4/EAC2PP
- FCS_RND.1/EAC2PP

325 The following SFRs are imported due to claiming [EAC1PP]. They concern cryptographic support for applications that contain EAC1-protected data groups.

- FCS_CKM.1/DH_PACE_EAC1PP
- FCS_CKM.4/EAC1_PP (equivalent to FCS_CKM.4/EAC2PP, listed here only for the sake of completeness)
- FCS_COP.1/PACE_ENC_EAC1PP
- FCS_COP.1/PACE_MAC_EAC1PP

326 *Application Note 28***:** Note that national regulations on key sizes and algorithms may further restrict the choice of algorithms and key sizes defined in the above two SFRs.

9 [assignment: *authorized users*]
10 [assignment: *list of audit information*]
11 [assignment: *authorized users*]
12 [assignment: *list of audit information*]

- FCS_RND.1/EAC1PP (equivalent to FCS_RND.1/EAC2PP, listed here only for the sake of completeness)
- FCS_CKM.1/CA_EAC1PP
- FCS_COP.1/CA_ENC_EAC1PP
- FCS_COP.1/SIG_VER_EAC1PP
- FCS_COP.1/CA_MAC_EAC1PP

327 The following SFRs are imported due to claiming [MREDONPP].

- FCS_CKM.1/UPD_ITC
- FCS_CKM.1/UPD_DEC
- FCS_CKM.1/UPD_INT
- FCS_CKM.4/UPD
- FCS_COP.1/UPD_ITC
- FCS_COP.1/UPD_DEC
- FCS_COP.1/UPD_SIG
- FCS_COP.1/UPD_INT

328 The following SFRs are imported due to claiming [SSCDPP]. They only concern the cryptographic support for an eSign application.

- FCS_CKM.1/SSCDPP
- FCS_CKM.4/SSCDPP (equivalent to FCS_CKM.4/EAC2PP, listed here only for the sake of completeness)
- FCS_COP.1/SSCDPP

329 The following SFRs are defined in [MREDPP] and concerns cryptographic support for enhancements of [EAC2PP] (Chip Authentication 3).

- FCS_CKM.1/CA3
- FCS_COP.1/CA3

330 The following SFRs are defined in [MREDPP] and concerns cryptographic support for ePassport applications in combination with [EAC1PP].

- FCS_CKM.1/CAM
- FCS_COP.1/CAM

331 The TOE provides cryptographic services based on elliptic curve cryptography (ECC) using the following curves with corresponding key lengths

(1) key length 192 bit
   a. brainpoolP192r1 defined in RFC5639 [RFC5639],
   b. brainpoolP192t1 defined in RFC5639 [RFC5639],
   c. ansix9p192r1 defined in ANSI X.9.62, identical to P-192 defined in [FIPS186],

(2) key length 224 bit
   a. brainpoolP224r1 defined in RFC5639 [RFC5639],
   b. brainpoolP224t1 defined in RFC5639 [RFC5639],

(3) key length 256 bit
   a. brainpoolP256r1 defined in RFC5639 [RFC5639],
   b. brainpoolP256t1 defined in RFC5639 [RFC5639],
   c. ansix9p256r1 defined in ANSI X.9.62, identical to P-256 defined in [FIPS186],

(4) key length 320 bit
   a. brainpoolP320r1 defined in RFC5639 [RFC5639],

b. brainpoolP320t1 defined in RFC5639 [RFC5639],

(5) key length 384 bit

a. brainpoolP384r1 defined in RFC5639 [RFC5639],
b. brainpoolP384t1 defined in RFC5639 [RFC5639],
c. ansix9p384r1 defined in ANSI X.9.62, identical to P-384 defined in [FIPS186],

(6) key length 512 bit

a. brainpoolP512r1 defined in RFC5639 [RFC5639].
b. brainpoolP512t1 defined in RFC5639 [RFC5639].

332 *Application Note 29*: Note that beside the listed supported elliptic curves, it is generally possible to import customer specific curves, if one follows the encoding rules defined in the TCOS Admin Guidance [TCOSGD]. Cryptographic security conditions, as e.g., required by [RFC5639, sec 2.1 Security Requirements], are not checked by the TOE. Therefore, it is strongly recommended to check the curve parameters before import during personalization phase by the administrator. The scope of the TOE contains only the specified curves. Because the curves with the length 192 and 224 are not specified in any SFR the scope of this TOE also does not include these curves.

333 FCS_CKM.1/CA_EAC1PP Cryptographic key generation – CA

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/CA_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to* [ECCTR][13] and specified cryptographic key sizes *256, 320, 384, 512 bit*[14] that meet the following: *based on an ECDH protocol compliant to TR-3110 [EACTR]*[15].

334 FCS_CKM.1/DH_PACE_EAC1PP Cryptographic key generation – DH by PACE

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/DH_PACE_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to*

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

14 [assignment: *cryptographic key sizes*]

15 [assignment: *list of standards*]

[ECCTR][16] and specified cryptographic key sizes *256, 320, 384, 512*[17] that meet the following: *TR-3110 [EACTR, part 2]*[18].

335 **FCS_CKM.1/DH_PACE_EAC2PP Cryptographic key generation – DH by PACE**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/DH_PACE_EAC2PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [ECCTR*[19] and specified cryptographic key sizes *256, 320, 384, 512*[20] that meet the following: TR-3110-2 [EACTR][21].

336 *Application Note 30***:** The TOE exchanges a shared secret with the external entity during the PACE protocol, see [EACTR]. This protocol is based on the ECDH protocol compliant to TR-03111 [ECCTR] (i.e. the elliptic curve cryptographic algorithm ECKA). The shared secret is used for deriving the AES session keys for message encryption and message authentication according to [EACTR] for the TSF as required by FCS_COP.1/ PACE.PICC.ENC, and FCS_COP.1/PACE.PICC.MAC. FCS_CKM.1/DH.PACE.PICC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to TR-03110 [EACTR].

337 **FCS_CKM.1/CA3 Cryptographic key generation – Diffie-Hellman for Chip Authentication 3**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/CA3

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Chip Authentication 3 using Diffie-Hellman[22] and specified cryptographic key sizes *256,*

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

17 [assignment: *cryptographic key sizes*]

18 [assignment: *list of standards*]

19 [selection: *id-PACE-ECDH-GM-AES-CBC-CMAC-128 with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 with brainpoolP512r1*]

20 [assignment: *cryptographic key sizes*]

21 [assignment: *list of standards*]

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

320, 384, 512[23] that meet the following: TR-03110-2 v.2.21[EACTR][24].

338 *Application Note 31:* After successful CA3, secure messaging (cf. FCS_COP.1/ PACE_\ ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP) is restarted using the derived session keys K_{Enc} and K_{MAC}.

339 FCS_CKM.1/CAM Cryptographic key generation – PACE-CAM public key and Diffie-Hellman for General Mapping in PACE-GM

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/CAM

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PACE-CAM in combination with PACE-GM[25] and specified cryptographic key sizes *256, 320, 384, 512*[26] that meet the following: [ICAO9303][27].

340 *Application Note 32:* In the combined protocol PACE-CAM, after the completion of PACE in combination with the general mapping (PACE-GM), the chip authenticates itself by adding (multiplying) the randomly chosen nonce of the GM step with the inverse of the chip authentication secret key, and sends this value together with chip authentication public key to the card; cf. [ICAO9303].

341 FCS_CKM.1/UPD_ITC Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/UPD_ITC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [ECCTR]*[28] and specified cryptographic key sizes *128,192,256 bit*[29] that meet the following: [*ECCTR*][30].

---

23 [assignment: *cryptographic key sizes*]

24 [assignment: *list of standards*]

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

26 [assignment: *cryptographic key sizes*]

27 [assignment: *list of standards*]

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

29 [assignment: *cryptographic key sizes*]

30 [assignment: *list of standards*]

342 *Application Note 33:* The details of the TCOS update mechanism are described in the TCOS Guidance.

343 FCS_CKM.1/UPD_DEC Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/UPD_DEC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECKA*[31] and specified cryptographic key sizes *256 bit*[32] that meet the following: [EACTR-3], [*TCOSGD*][33].

344 FCS_CKM.1/UPD_INT Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/UPD_INT

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *none*[34] and specified cryptographic key sizes *none*[35] that meet the following: *none*[36].

345 *Application Note 34:* The integrity is solely implied by a digital signature verification; hence no key is used here.

346 FCS_CKM.1/SSCDPP Cryptographic key generation – SSCD

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_CKM.1.1/SSCDPP

---

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

32 [assignment: *cryptographic key sizes*]

33 [assignment: *list of standards*]

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

35 [assignment: *cryptographic key sizes*]

36 [assignment: *list of standards*]

The TSF shall generate **an SCD/SVD pair** ~~cryptographic keys~~ in accordance with a specified cryptographic key generation algorithm *EC-DSA key generation compliant to* [*ECCTR*][37] and specified cryptographic key sizes *256, 320, 384 and 512 bit length group order*[38] that meet the following: [*ECCTR*][39].

347 **FCS_CKM.4/EAC2PP 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

FCS_CKM.4.1/EAC2PP

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*[40] that meets the following: *none*[41].

348 *Application Note 35:* The TOE destroys encryption session keys, and the message authentication keys for secure messaging and the PACE protocol after reset or termination of secure messaging session (trusted channel) or reaching fail secure state according to FPT_FLS.1. The TOE clears the memory area of any session keys before starting a new communication with an external entity in a new after-reset-session as required by FDP_RIP.1.

349 *Application Note 36:* This SFR also covers the iterated FCS_CKM.4/SSCDPP using the same Selections. The destruction of the SCD is done at least on demand of the signatory using the Terminate-command. S.User with the security attribute ‘Role’ set to ‘R.Sigy’ is allowed to destroy the SCD.

350 **FCS_CKM.4/UPD 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

FCS_CKM.4.1/UPD

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

38 [assignment: *cryptographic key sizes*]

39 [assignment: *list of standards*]

40 [assignment: *cryptographic key destruction method*]

41 [assignment: *list of standards*]

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*[42] that meets the following: *none*[43].

351 **FCS_COP.1/CA_ENC_EAC1PP Cryptographic operation**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/CA_ENC_EAC1PP

The TSF shall perform secure messaging – encryption and decryption[44] in accordance with a specified cryptographic algorithm *AES in CBC mode*[45] and cryptographic key sizes *128, 192 and 256 bit* [46] that meet the following: *compliant to* [ICAOSAC][47].

352 **FCS_COP.1/CA_MAC_EAC1PP Cryptographic operation**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/CA_MAC_EAC1PP

The TSF shall perform secure messaging – message authentication code[48] in accordance with a specified cryptographic algorithm *CMAC(AES)*[49] and cryptographic key sizes *128, 192 or 256 bit*[50] that meet the following: *compliant to* [ICAOSAC][51].

353 **FCS_COP.1/CAM PACE-CAM**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

42 [assignment: *cryptographic key destruction method*]

43 [assignment: *list of standards*]

44 [assignment: *list of cryptographic operations*]

45 [assignment: *cryptographic algorithm*]

46 [assignment: *cryptographic key sizes*]/[selection: 112, 128, 192, 256]

47 [assignment: *list of standards*]

48 [assignment: *list of cryptographic operations*]

49 [assignment: *cryptographic algorithm*]

50 [assignment: *cryptographic key sizes*]/[selection: 112, 128, 192, 256] bit

51 [assignment: *list of standards*]

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation] fulfilled

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/CAM

The TSF shall perform the PACE-CAM protocol[52] in accordance with a specified cryptographic algorithm PACE-CAM[53] and cryptographic key sizes *256, 320, 384, 512 bit*[54] that meet the following: [EACTR, part 2][55].

354 **FCS_COP.1/PACE_ENC_EAC1PP Cryptographic operation – PACE secure messaging encryption**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/PACE_ENC_EAC1PP

The TSF shall perform decryption and encryption for secure messaging[56]in accordance with a specified cryptographic algorithm *AES*[57] in CBC mode[58] and cryptographic key sizes *128, 192, 256 bit*[59] that meet the following: compliant to TR-03110 [EACTR, part 2][60].

355 *Application Note 37:* This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE.

356 **FCS_COP.1/PACE_ENC_EAC2PP Cryptographic operation – PACE secure messaging encryption**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/PACE_ENC_EAC2PP

52 [assignment: *list of cryptographic operations*]

53 [assignment: *cryptographic algorithm*]

54 [assignment: *cryptographic key sizes*]/[selection: 112, 128, 192, 256] bit

55 [assignment: *list of standards*]

56 [assignment: *list of cryptographic operations*]

57 [selection: *AES,3DES*]

58 [assignment: *cryptographic algorithm*]

59 [assignment: *cryptographic key sizes*]

60 [assignment: *list of standards*]

The TSF shall perform secure messaging - encryption and decryption [61]in accordance with a specified cryptographic algorithm AES in CBC mode[62] and cryptographic key sizes *128, 192, 256 bit*[63] that meet the following: **TR-03110 [EACTR, part 3]**[64].

357 *Application Note 38***:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE.

358 FCS_COP.1/PACE_MAC_EAC1PP Cryptographic operation – PACE secure messaging 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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/PACE_MAC_EAC1PP

The TSF shall perform MAC calculation for secure messaging[65] in accordance with a specified cryptographic algorithm *CMAC(AES)*[66] and cryptographic key sizes *128 bit, 192 bit, 256 bit*[67] that meet the following: compliant to [ICAOSAC][68].

359 *Application Note 39:* This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data.

360 FCS_COP.1/PACE_MAC_EAC2PP Cryptographic operation – PACE secure messaging 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

FCS_CKM.4 Cryptographic key destruction fulfilled

61 [assignment: *list of cryptographic operations*]

62 [assignment: *cryptographic algorithm*]

63 [assignment: *cryptographic key sizes*]

64 [assignment: *list of standards*]

65 [assignment: *list of cryptographic operations*]

66 [assignment: *cryptographic algorithm*]

67 [assignment: *cryptographic key sizes*]

68 [assignment: *list of standards*]

FCS_COP.1.1/PACE_MAC_EAC2PP

The TSF shall perform MAC calculation for secure messaging[69] in accordance with a specified cryptographic algorithm CMAC(AES)[70] and cryptographic key sizes *128 bit, 192 bit, 256 bit*[71] that meet the following: **TR03110-3[EACTR, part 3]**[72].

361 *Application Note 40*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data.

362 FCS_COP.1/SHA_EAC2PP Cryptographic operation – SHA

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] justified in [MREDPP]: the dependent SFRs are not applicable because this SFR does not use any keys.

FCS_CKM.4 Cryptographic key destruction justified in [MREDPP]: the dependent SFRs are not applicable because this SFR does not use any keys.

FCS_COP.1.1/SHA_EAC2PP

The TSF shall perform hashing[73] in accordance with a specified cryptographic algorithm

(1) SHA-1,
(2) SHA-224,
(3) SHA-256,
(4) SHA-384,
(5) *SHA-512* [74]

and cryptographic key sizes none[75] that meet the following: FIPS 180-4 [FIPS180][76].

363 FCS_COP.1/SIG_VER_EAC1PP 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]

69 [assignment: *list of cryptographic operations*]
70 [assignment: *cryptographic algorithm*]
71 [assignment: *cryptographic key sizes*]
72 [assignment: *list of standards*]
73 [assignment: *list of cryptographic operations*]
74 [assignment: *cryptographic algorithm*]
75 [assignment: *cryptographic key sizes*]
76 [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/ SIG_VER_EAC1PP

The TSF shall perform digital signature verification[77] in accordance with a specified cryptographic algorithm *ECDSA with plain signature format*[78] and cryptographic key sizes *256, 320, 384 and 512 bit length group order*[79] that meet the following: [*EACTR*][80].

364 **FCS_COP.1/SIG_VER_EAC2PPCryptographic 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} (initialization data) used for verifying the DV Certificate is stored in the TOE during its personalization in the card issuing life cycle phase 7. Since importing the respective certificates (Terminal Certificate, DV Certificate) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the EAC2PP does not contain any dedicated requirement like FDP_ITC.2 for the import function.

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/SIG_VER_EAC2PP

The TSF shall perform digital signature verification[81] in accordance with a specified cryptographic algorithm *ECDSA with plain signature format*[82] and cryptographic key sizes *256, 320, 384 and 512 bit length group order*[83] that meet the following: [*EACTR*][84].

365 **FCS_COP.1/CA3 Cryptographic operation – CA3**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/CA3

77 [assignment: *list of cryptographic operations*]

78 [assignment: *cryptographic algorithm*]

79 [assignment: *cryptographic key sizes*]

80 [assignment: *list of standards*]

81 [assignment: *list of cryptographic operations*]

82 [assignment: *cryptographic algorithm*]

83 [assignment: *cryptographic key sizes*]

84 [assignment: *list of standards*]

The TSF shall perform the Chip authentication 3 (CA3) protocol[85] in accordance with a specified cryptographic algorithm CA3[86] and cryptographic key sizes *256, 320, 384, 512 bit*[87] that meet the following: TR03110-2-v2.21 [EACTR][88].

366 *Application Note 41*: Whereas FCS_CKM.1/CA3 addresses the Diffie-Hellman based key-derivation, this SFR is concerned with the correct implementation and execution of the whole CA3 protocol. This in particular includes pseudonymous signature generation with PSign [EACTR].

367 FCS_COP.1/UPD_ITC Cryptographic operation – Inter Trusted Channel

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/UPD_ITC

The TSF shall perform *signature verification*[89] in accordance with a specified cryptographic algorithm *EC-DSA*[90] and cryptographic key sizes *512 bit*[91] that meet the following: [*ECCTR*][92].

368 *Application Note 42*: The integrity of the trusted channel is protected by a digital signature over a hash value of chained MAC values computed during the update procedure. Only the curve BrainpoolP512T1 is used here.

369 FCS_COP.1/UPD_DEC Cryptographic operation – Decryption of Update Packages

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/UPD_DEC

The TSF shall perform decryption of update packages[93] in accordance with a specified cryptographic algorithm *AES-256 in OFB*

85 [assignment: *list of cryptographic operations*]

86 [assignment: *cryptographic algorithm*]

87 [assignment: *cryptographic key sizes*]

88 [assignment: *list of standards*]

89 [assignment: *list of cryptographic operations*]

90 [assignment: *cryptographic algorithm*]

91 [assignment: *cryptographic key sizes*]

92 [assignment: *list of standards*]

93 [assignment: *list of cryptographic operations*]

mode[94] and cryptographic key sizes *256 bit*[95] that meet the following: [*FIPS197*] and [*SP800-38A*][96].

370 **FCS_COP.1/UPD_INT Cryptographic operation – Integrity Verification of Update Package**

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

FCS_COP.1.1/UPD_INT

The TSF shall perform integrity verification of update packages[97] in accordance with a specified cryptographic algorithm *SHA256*[98] and cryptographic key sizes *none*[99] that meets the following: *[FIPS197]*[100].

371 *Application Note 43*: The whole Update Package is protected by a digital signature of a hash value, and therefore no key is used here.

372 **FCS_COP.1/UPD_SIG Cryptographic operation – Signature Verification of Update Packages**

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 [MREDONPP]

FCS_CKM.4 Cryptographic key destruction not fulfilled but justified [MREDONPP]

FCS_COP.1.1/UPD_SIG

The TSF shall perform digital signature verification[101] in accordance with a specified cryptographic algorithm *EC-DSA*[102] and cryptographic key sizes *512 bit*[103] that meet the following: *[TCOSGD]*[104].

373 *Application Note 44*: Only the curve BrainpoolP512T1 is used here.

---

94 [assignment: *cryptographic algorithm*]

95 [assignment: *cryptographic key sizes*]

96 [assignment: *list of standards*]

97 [assignment: *list of cryptographic operations*]

98 [assignment: *cryptographic algorithm*]

99 [assignment: *cryptographic key sizes*]

100 [assignment: *list of standards*]

101 [assignment: *list of cryptographic operations*]

102 [assignment: *cryptographic algorithm*]

103 [assignment: *cryptographic key sizes*]

104 [assignment: *list of standards*]

374 **FCS_COP.1/SSCDPP Cryptographic operation – Qualified Signature Creation**

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

FCS_CKM.4 Cryptographic key destruction fulfilled

FCS_COP.1.1/SSCDPP

The TSF shall perform digital signature generation[105] in accordance with a specified cryptographic algorithm *EC-DSA compliant to* [*EC-CTR*][106] and cryptographic key sizes *256, 320, 384 and 512 bit length group order*[107] that meet the following: [*ECCTR*][108].

375 **FCS_RND.1/EAC2PP Random number generation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1 Random number generation (Class PTG.3)

FCS_RND.1.1/EAC2PP

The TSF shall provide a *hybrid physical*[109] random number generator that implements:

(PTG.3.1) *A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output*.

(PTG.3.2) *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*[110].

(PTG.3.3) *The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.*

105 [assignment: *list of cryptographic operations*]

106 [assignment: *cryptographic algorithm*]

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

108 [assignment: *list of standards*]

109 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

110 [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 inter-nal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy*]

(PTG.3.4) *The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon*.

(PTG.3.5) *The online test procedure checks the raw random number sequence. It is triggered continuously*[111]*. 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.*

(PTG.3.6) *The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.*

FCS_RND.1.2/EAC2PP

The TSF shall provide *octets of bits*[112] that meet:

(PTG.3.7) *Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.*

(PTG.3.8) *The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing*[113]*.*

6.1.4 Class FIA Identification and Authentication

376 The following Table provides an overview of the authentication and identification mechanisms used.

377 The following SFRs are imported due to claiming [EAC2PP]. They mainly concern authentication mechanisms related to applications with EAC2-protected data.

- FIA_AFL.1/Suspend_PIN_EAC2PP
- FIA_AFL.1/Block_PIN_EAC2PP
- FIA_API.1/CA_EAC2PP
- FIA_API.1/RI_EAC2PP
- FIA_UID.1/PACE_EAC2PP
- FIA_UID.1/EAC2_Terminal_EAC2PP

378 *Application Note 45*: The user identified after a successfully performed TA2 protocol is an EAC2 terminal. Note that TA1 is covered by FIA_UID.1/PACE_EAC1PP. In that case, the terminal identified is in addition also an EAC1 terminal.

- FIA_UAU.1/PACE_EAC2PP
- FIA_UAU.1/EAC2_Terminal_EAC2PP
- FIA_UAU.4/PACE_EAC2PP
- FIA_UAU.5/PACE_EAC2PP
- FIA_UAU.6/CA_EAC2PP
- FIA_AFL.1/PACE_EAC2PP
- FIA_UAU.6/PACE_EAC2PP

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

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

113 [selection: *use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work]]*.

379 The following SFRs are imported due to claiming [EAC1PP]. They mainly concern authentication mechanisms for applications with EAC1-protected data.

- FIA_UID.1/PACE_EAC1PP
- FIA_UAU.1/PACE_EAC1PP
- FIA_UAU.4/PACE_EAC1PP
- FIA_UAU.5/PACE_EAC1PP
- FIA_UAU.6/PACE_EAC1PP (equivalent to FIA_UAU.6/PACE_EAC2PP, listed here only for the sake of completeness)
- FIA_UAU.6/EAC_EAC1PP
- FIA_API.1/EAC1PP
- FIA_AFL.1/PACE_EAC1PP (equivalent to FIA_AFL.1/PACE_EAC2PP, listed here only for the sake of completeness)

380 The following SFRs are defined in [MREDPP] and concern enhancements of [EAC2PP] (Chip Authentication 3).

- FIA_API.1/CA3
- FIA_API.1/PACE_CAM
- FIA_UAU.6/CA3

381 The following SFRs are imported due to claiming [MREDONPP].

- FIA_AFL.1/UPD
- FIA_UAU.1/UPD
- FIA_UID.1/UPD

382 The following SFRs are imported due to claiming [SSCDPP]. They concern access mechanisms for an eSign application, if available.

- FIA_UID.1/SSCDPP
- FIA_AFL.1/SSCDPP

383 **FIA_AFL.1/Suspend_PIN_EAC2PP Authentication failure handling – Suspending PIN**

Hierarchical to: No other components.

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

FIA_AFL.1.1/Suspend_PIN_EAC2PP

The TSF shall detect when *2*[114] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using PIN as the shared password for PACE[115].

FIA_AFL.1.2/Suspend_PIN_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[116], the TSF shall suspend the reference value of PIN according to [EACTR-2][117].

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

115 [assignment: *list of authentication events*]

116 [selection: *met, surpassed*]

117 [assignment: *list of actions*]

384 *Application Note 46:* According to [**EACTR**] at least the current value 1 of the retry counter for PIN shall be a suspending value, i.e. if this value is reached the 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 [TCOSGD].

385 **FIA_AFL.1/Block_PIN_EAC2PPAuthentication failure handling – Blocking PIN**

Hierarchical to: No other components.

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

FIA_AFL.1.1/Block_PIN_EAC2PP

The TSF shall detect when *1*[118] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using suspended PIN as the shared password for PACE[119].

FIA_AFL.1.2/Block_PIN_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[120], the TSF shall block the reference value of PIN according to [EACTR-2][121].

386 *Application Note 47:* According to [EACTR-2], the 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 PIN shall be RC = 0.

387 **FIA_AFL.1/PACE_EAC2PP 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/PACE_EAC2PP

The TSF shall detect when *1*[122] unsuccessful authentication attempt~~s~~ occur**s** related to authentication attempts using PACE password as shared password[123].

FIA_AFL.1.2/PACE_EAC2PP

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

119 [assignment: *list of authentication events*]

120 [selection: *met, surpassed*]

121 [assignment: *list of actions*]

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

123 [assignment: *list of authentication events*]

When the defined number of unsuccessful authentication attempts has been met[124], the TSF shall *require the restart of the PACE protocol; and the TSF will increase the reaction time to the next authentication attempt*[125].

388 *Application Note 48:* The assignment operation reflects the fact that according the implementation the authentication procedure consumes a defined minimal amount of time. Because MRZ and PUK possesses enough entropy for this reaction time (cf. Administrator Guidance [TCOSGD]), 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, 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.

389 *Application Note 49:* The TOE detects any unsuccessful authentication attempt. After 32 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. [TCOSGD]).

390 FIA_AFL.1/UPD Update Package Verification Failure Handling

Hierarchical to: No other components.

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

FIA_AFL.1.1/UPD

The TSF shall detect when *1*[126] unsuccessful ~~authentication~~ **update attempt~~s~~** occur~~s~~ related to *mutual authentication of the TCOS update procedure*[127].

FIA_AFL.1.2/UPD

When the defined number of unsuccessful ~~authentication~~ **update attempts** has been met[128], the TSF shall *require the restart of the update procedure*[129].

391 *Application Note 50:* The above SFR is slightly refined here by replacing 'authentication' with 'update'. In addition, the second assignment is made more precise. An update attempt includes authentication of the update terminal to the TOE. However, when a properly authenticated terminal sends an update package that is not authentic or whose integrity cannot be validated, this is still a failed update attempt and the TOE handles it according to the above SFR. Hence, this refinement is stricter than the original SFR definition.

392 FIA_API.1/CA_EAC2PP Authentication Proof of Identity

Hierarchical to: No other components.

---

124 [selection: *met, surpassed*]

125 [assignment: *list of actions*]

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

127 [assignment: *list of ~~authentication~~ events of the update procedure*]

128 [selection: *met, surpassed*]

129 [assignment: *list of actions*]

Dependencies: No dependencies.

FIA_API.1.1/CA_EAC2PP

The TSF shall provide the Chip Authentication Protocol according to [EACTR-2 Version 2 (for GAP)][130] to prove the identity of the TOE[131].

393 *Application Note 51:* The Chip Authentication shall be triggered by the terminal immediately after the successful Terminal Authentication (as required FIA_UAU.1/EAC2_Terminal_EAC2PP) using, amongst other, H(ephem-PKPCD-TA) from the accomplished TA. The terminal verifies genuineness of the ID Card by verifying the authentication token TPICC calculated by the TOE using ephem-PKPCD-TA and CA-KMAC, (and, hence, finally making evident possessing the Chip Authentication Key (SKPICC)).

394 The Passive Authentication making evident authenticity of the PKPICC by verifying the Card/Chip Security Object (SOC) up to CSCA shall be triggered by the rightful terminal immediately after the successful Terminal Authentication before the Chip Authentication and is considered to be part of the CA Protocol (see also P.Terminal).

395 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-KMAC, CA-KEnc), cf. FTP_ITC.1/CA_\ EAC2PP. Otherwise, Secure Messaging is continued using the previously established session keys (PACE-KMAC, PACE-KEnc), cf. FTP_ITC.1/PACE.

396 Please note that the Chip Authentication Protocol according to [EACTR-2, 3.3], version 1 (for AIP) is covered by FIA_API.1 there.

397 FIA_API.1/CA3 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA3

The TSF shall provide the protocol Chip Authentication 3 according to [EACTR-2][132] to prove the identity of the TOE[133].

398 FIA_API.1/PACE_CAM Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CAM

The TSF shall provide the protocol PACE-CAM [ICAO9303][134], to prove the identity of the TOE[135].

130 [assignment: *authentication mechanism*]

131 [assignment: *authorized user or role*]

132 [assignment: *authentication mechanism*]

133 [assignment: *authorized user or role*]

134 [assignment: *authentication mechanism*]

135 [assignment: *authorized user or role*]

399 **FIA_API.1/RI_EAC2PP Authentication Proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/RI_EAC2PP

The TSF shall provide the Restricted Identification protocol according to [EACTR-2][136] to prove the identity of the TOE[137].

400 *Application Note 52*: The Restricted Identification provides a sector-specific identifier of every electronic document. It thus provides a pseudonymous way to identify the electronic document holder in a case where the CHAT of the terminal does not allow to access sensitive user data that directly identify the electronic document holder. Restricted Identification shall only be used after successfully running Terminal Authentication 2 and Chip Authentication 2. Note that Restricted Identification is optional according to [EACTR-2], and thus the above SFR only applies if Restricted Identification is supported by the TOE.

401 **FIA_API.1/EAC1PP Authentication Proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/EAC1PP

The TSF shall provide the Chip Authentication Protocol according to [EACTR-2][138] to prove the identity of the TOE[139].

402 *Application Note 53:* In [EACTR-2, 3.3] the Chip Authentication Mechanism 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).

403 **FIA_UID.1/PACE_EAC2PPTiming of identification**

404 This SFR is refined from [EAC1PP]. Refinements address the PACE-CAM protocol.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE_EAC2PP

The TSF shall allow

1. to establishing a communication channel,
2. carrying out the PACE Protocol according to **[EACTR-2]**,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. *none* [140].

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

136 [assignment: *authentication mechanism*]

137 [assignment: *authorized user or role*]

138 [assignment: *authentication mechanism*]

139 [assignment: *authorized user or role*]

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

FIA_UID.1.2/PACE_EAC2PP

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

405 *Application Note 54:* The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK were used for PACE, the user identified is the electronic document holder using a PACE terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the electronic document holder itself, an authorized person other than the electronic document holder, or a device.

406 **FIA_UID.1/EAC2_Terminal_EAC2PP Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/EAC2_Terminal_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [EACTR-2],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. carrying out the Terminal Authentication Protocol 2 protocol according to [EACTR-2]
5. *none*[141].

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

FIA_UID.1.2/EAC2_Terminal_EAC2PP

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

407 *Application Note 55:* The user identified after a successfully performed TA protocol is a terminal for GAP: either EIS-GAP or ATT or SGT.

408 *Application Note 56:* 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.

409 Please note that a Personalization Agent acts on behalf of the 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-3, C.4, Table 21].

410 **FIA_UID.1/PACE_EAC1PP Timing of identification**

411 This SFR is refined from [EAC1PP]. Refinements address the PACE-CAM protocol.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE_EAC1PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE Protocol according to **[EACTR-1]**,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to carry out either the Chip Authentication Protocol v.1 according to [EACTR-1] **or the Chip Authentication Mapping (PACE-CAM) according to [ICAO9303]**,
5. to carry out the Terminal Authentication Protocol v.1 according to [EACTR-1] **resp. according to [ICAO9303] if PACE-CAM is used**
6. *none*[142].

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

FIA_UID.1.2/PACE_EAC1PP

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

412 *Application Note 57:* The user identified after a successfully performed PACE protocol is a PACE terminal (PCT). In case PIN or PUK were used for PACE, it is the ID_Card holder using PCT. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. in case CAN or MRZ were used for PACE, it is either the RP_Card holder itself or an authorized other person or device.

413 FIA_UAU.1/PACE_EAC2PP 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_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE Protocol[143] according to **[EACTR-2]**
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. *none*[144]

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

FIA_UAU.1.2/PACE_EAC2PP

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

143 electronic document identifies themselves within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

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

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

414 *Application Note 58:* The user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). In case PIN or 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.

415 FIA_UAU.1/EAC2_Terminal_EAC2PP Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/EAC2_Terminal_EAC2PP.

FIA_UAU.1.1/EAC2_Terminal_EAC2PP

The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE protocol according to [EACTR-2, 3.2],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. carrying out the Terminal Authentication Protocol 2 protocol according to [EACTR-2][145]

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

FIA_UAU.1.2/EAC2_Terminal_EAC2PP

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

416 *Application Note 59:* The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated terminal will immediately perform Chip Authentication 2 as required by FIA_API.1/CA using, amongst other, Comp(ephem-PK_{PCD}-TA) from the accomplished TA2. Note that Passive Authentication using SO_C is considered to be part of CA2 protocol.

417 FIA_UAU.1/PACE_EAC1PP 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_EAC1PP

The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE Protocol[146] according to [EACTR-1],

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

146 electronic document identifies themselves within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol Version 1 according to [EACTR-1],
6. to carry out the Terminal Authentication Protocol Version 1 according to [EACTR-1]
7. *none*[147]

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

FIA_UAU.1.2/PACE_EAC1PP

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

418 **FIA_UID.1/UPD Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/UPD

The TSF shall allow

1. to establish a communication channel,
2. to authenticate an update terminal by the *TA2 protocol according to* [EACTR-2][148],
3. *none*[149].

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

FIA_UID.1.2/UPD

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

419 **FIA_UAU.1/UPD Timing of authentication**

Hierarchical to: No other components.

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

FIA_UAU.1.1/UPD

The TSF shall allow

1. to establish a communication channel,
2. to authenticate an update terminal by the *TA2 protocol according to* [EACTR-2][150],
3. *none*[151].

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

148 [assignment: *cryptographic method*]

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

150 [assignment: *cryptographic method*]

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

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

FIA_UAU.1.2/UPD

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

420 **FIA_UAU.4/PACE_EAC2PP 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/PACE_EAC2PP

The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to [EACTR-2, 3.2],
2. Authentication Mechanism based on *AES*[152]
3. Terminal Authentication 2 protocol according to [EACTR-2, 3.4],
4. *none*[153].

421 *Application Note 60:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits Length being (almost) uniformly distributed. For the TA protocol, TOE randomly selects a nonce r_{PICC} of 64 bits length, see [EACTR-3, B.3 and B.11.6].

422 **FIA_UAU.4/PACE_EAC1PP 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/PACE_EAC1PP

The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to **[EACTR-1]**,
2. Authentication Mechanism based on *AES*[154],
3. Terminal Authentication Protocol v1 according to [EACTR-1][155].

423 **FIA_UAU.5/PACE_EAC2PP Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE_EAC2PP

---

152 [selection: ~~*Triple-DES*~~ *, AES or other approved algorithms*]

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

154 [selection: *Triple-DES, AES or other approved algorithms*]

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

The TSF shall provide

1. PACE protocol according to **[EACTR-2]**,
2. Passive Authentication according to [ICAO9303],
3. Secure messaging ~~**in MAC-ENC mode**~~ according to **[EACTR-3]**
4. Symmetric Authentication Mechanism based on *AES*[156],
5. Terminal Authentication 2 protocol according to [EACTR-2],
6. Chip Authentication 2 according to [EACTR-2][157],
7. Chip Authentication 3 according to [EACTR-2-v2.20],
8. *none* [158]

to support user authentication.

FIA_UAU.5.2/PACE_EAC2PP

The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol
2. The TOE accepts the authentication attempt as personalization agent by *the Authentication Mechanism with Personalization Agent Key(s)* [159]
3. The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PK_{PCD} and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier ID_{PICC} = Comp(ephem-PK_{PICC}-PACE) calculated during, and the secure messaging established by the, current PACE authentication,
4. Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.
5. Having successfully run Chip Authentication 3, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 3,
6. *none*[160].

424 *Application Note 61:* 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.

425 Please note that the Chip Authentication Protocol according to [EACTR-2, sec. 3.3], version 1 (for AIP) is covered in this context by [EAC1PP] (see FIA_UAU.5 there).

156 [selection: *AES or other approved algorithms*]

157 Passive Authentication using SOC is considered to be part of CA2

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

159 [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]

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

426 *Application Note 62:* 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.

427 **FIA_UAU.5/PACE_EAC1PP Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE_EAC1PP

The TSF shall provide

1. PACE Protocol **and PACE-CAM protocol according to [ICAO9303],**
2. Passive Authentication according to [ICAO9303],
3. Secure messaging in MAC-ENC mode according to [ICAO9303],
4. Symmetric Authentication Mechanism based on *AES*[161]
5. Terminal Authentication Protocol v.1 according to [EACTR-1]

to support user authentication[162].

FIA_UAU.5.2/PACE_EAC1PP

The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE 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 PACE protocol.
2. The TOE accepts the authentication attempt as Personalization Agent by *the Authentication Mechanism with Personalization Agent Key(s)*[163].
3. After run of the Chip Authentication Protocol Version 1 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 v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 **, or if the terminal uses the public key presented during PACE-CAM and the secure messaging established during PACE**[164]
5. *none*[165].

161 [selection: *Triple-DES, AES or other approved algorithms*]

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

163 [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]

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

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

428 The PP ([PACEPP]) 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.

429 FIA_UAU.6/CA3 Re-Authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/CA3

The TSF shall re-authenticate the user under the conditions~~s~~ each command sent to the TOE after successful run of the Chip Authentication 3 shall be verified as being sent by the EAC2 terminal[166].

430 FIA_UAU.6/CA_EAC2PP Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/CA_EAC2PP

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication 2 shall shall be verified as being sent by the EAC2 terminal[167].

431 FIA_UAU.6/PACE_EAC2PP Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE_EAC2PP

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal[168].

432 *Application Note 63:* The PACE protocol specified in [EACTR] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC 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.

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

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

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

433 **FIA_UAU.6/EAC_EAC1PP Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC_EAC1PP

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System[169].

434 *Application Note 64:* The PACE and the Chip Authentication Protocols specified in [EACTR] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

435 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/SSCDPP	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.
FIA_UID.1/SSCDPP	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.
FIA_AFL.1/SSCDPP	–	This requirement concerns the dedicated authentication data for the eSign application like eSign-PIN and eSign-PUK, if any.

436 **FIA_UAU.1/SSCDPP Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/SSCDPP, cf. [SSCDPP]

FIA_UAU.1.1/SSCDPP

The TSF shall allow

1. self test according to FPT_TST.1/SSCDPP,
2. identification of the user by means of TSF required by FIA_UID.1/SSCDPP

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

3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2 and FTP_\ ITC.1/CA3 respectively[170],
4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2 and FTP_\ ITC.1/CA3 respectively [171],
5. *none*[172]

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

FIA_UAU.1.2/SSCDPP

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

437 FIA_UID.1/SSCDPP Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/SSCDPP

The TSF shall allow

1. self test according to FPT_TST.1,
2. *none* [173]

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

FIA_UID.1.2/SSCDPP

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

438 FIA_AFL.1/SSCDPP Authentication failure handling

Hierarchical to: No other components.

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

FIA_AFL.1.1/SSCDPP

The TSF shall detect when *3*[174] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[ITC175].

FIA_AFL.1.2/SSCDPP

---

170 the authenticated terminal is ATT, cf. FIA_UAU.1/EAC2_Terminal

171 the authenticated terminal is SGT, cf. FIA_UAU.1/EAC2_Terminal; the trusted channel by FTP_ITC.1/CA implements a trusted path between HID and the TOE

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

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

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

175 [assignment: *list of authentication events*]

When the defined number of unsuccessful authentication attempts has been met[176], the TSF shall block RAD[177].

6.1.5 Class FDP User Data Protection

439 Multiple iterations of FDP_ACF.1 exist from imported PPs to define the access control SFPs for (common) user data, EAC1-protected user data, and EAC2-protected user data. The access control SFPs defined in FDP_ACF.1/EAC1PP from [EAC1PP] and FDP_ACF.1/EAC2PP from [EAC2PP] are here unified to one single FDP_ACF.1/TRM, whereas the several iterations of FDP_ACF.1 from [SSCDPP] stand separate. Here we take FDP_ACF.1/EAC2PP as a base definition of functional elements, and it is refined in a way that it is compatible with FDP_ACF.1/EAC1PP. Hence highlighting refers to changes w.r.t. to FDP_ACF.1/EAC2PP. In the Application Note below, we explain how FDP_ACF.1/EAC1PP is covered as well.

440 Concerning FDP_ACF.1/TRM here and the several iterations FDP_ACF.1 from [SSCDPP], we remark that FDP_ACF.1/TRM also concerns data and objects for signature generation. Note however, that FDP_ACF.1/TRM requires that prior to granting access to the signature application, in which the access controls defined in [SSCDPP] apply, an EAC2 terminal and the electronic document holder need to be authenticated. Hence, no inconsistency exists.

441 The following SFRs are imported due to claiming [EAC2PP]. They concern access control mechanisms related to EAC2-protected data.

- FDP_ACC.1/TRM_EAC2PP This SFR is equivalent to/covered by FDP_ACC.1/TRM_EAC1PP; cf. the Application Note above.
- FDP_ACF.1/TRM_EAC2PP This SFR is equivalent to/covered by FDP_ACF.1/TRM
- FDP_RIP.1/EAC2PP
  Application Note 65: Note that the formulation session keys in the above SFR MUST be interpreted here to include CA3 ephemeral and session keys as well..
- FDP_UCT.1/TRM_EAC2PP
- FDP_UIT.1/TRM_EAC2PP

442 The following SFRs are imported due to claiming [EAC1PP]. They concern access control mechanisms related to EAC1-protected data.

- FDP_ACC.1/TRM_EAC1PP The above is equivalent to FDP_ACC.1/TRM_EAC2PP, since EF.SOD (cf. FDP_ACC.1/TRM in [EAC1PP]) can be considered user data.; cf. also the Application Note below FDP_ACF.1/TRM.
- FDP_ACF.1/TRM_EAC1PP The above is covered by FDP_ACF.1/TRM; cf. *Application Note* there.
- FDP_RIP.1/EAC1PP
- FDP_UCT.1/TRM_EAC1PP (equivalent to FDP_UCT.1/TRM_EAC2PP, listed here only for the sake of completeness)
- FDP_UIT.1/TRM_EAC1PP (equivalent to FDP_UIT.1/TRM_EAC2PP, listed here only for the sake of completeness)

443 The following SFRs are imported due to claiming [MREDONPP].

- FDP_ACC.1/UPD
- FDP_ACF.1/UPD

176 [selection: *met, surpassed*]

177 [assignment: *list of actions*]

- FDP_IFC.1/UPD
- FDP_IFF.1/UPD
- FDP_RIP.1/UPD

444 The following SFRs are imported due to claiming [SSCDPP]. They concern access control mechanisms of an eSign application.

- FDP_ACC.1/SCD/SVD_Generation_SSCDPP
- FDP_ACF.1/SCD/SVD_Generation_SSCDPP
- FDP_ACC.1/SVD_Transfer_SSCDPP
- FDP_ACF.1/SVD_Transfer_SSCDPP
- FDP_ACC.1/Signature-creation_SSCDPP
- FDP_ACF.1/Signature-creation_SSCDPP
- FDP_RIP.1/SSCDPP
- FDP_SDI.2/Persistent_SSCDPP
- FDP_SDI.2/DTBS_SSCDPP

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled

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 Access Control SFP[178] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. PACE Terminal,
   c. EAC2 terminal: *EIS, ATT, SGT* [179]
   d. EAC1 terminal
2. Objects:
   a. all user data stored in the TOE; including sensitive **EAC1-protected user data, and sensitive EAC2-protected** user data,
   b. all TOE intrinsic secret (cryptographic) data
3. Security attributes:
   a. Terminal Authorization Level (access rights)
   b. Authentication status of the electronic document holder as a signatory (if an eSign application is included)[180].

178 [assignment: *access control SFP*]

179 [assignment: *list of EAC2 terminal types*]

180 [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*]

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:

A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful PACE authentication according to [EACTR-2] **and/or [ICAO9303]**, as required by FIA_UAU.1/PACE[181].

FDP_ACF.1.3/TRM

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[182].

FDP_ACF.1.4/TRM

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. Any terminal not being ~~authenticated as~~ a PACE terminal or an EAC2 terminal **or an EAC1 terminal** is not allowed to read, to write, to modify, to use any User Data stored on the electronic document.
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document.
3. No subject is allowed to read 'Communication Establishment Authorization Data' stored on the electronic document
4. No subject is allowed to write or modify 'secret electronic document holder authentication data' stored on the electronic document, except for PACE terminals or EAC2 terminals executing PIN management based on the following rules: *Change PIN, Resume PIN, Unblock PIN, Activate PIN, Deactivate PIN*[183]
5. No subject is allowed to read, write, modify, or use the private Restricted Identification key(s) and Chip Authentication key(s) stored on the electronic document.
6. Reading, modifying, writing, or using sensitive user data **that are protected only by EAC2, is allowed only** to EAC2 terminals using the following mechanism: The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to [EACTR-2] . To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE

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

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

183 [assignment: *list of rules for PIN management chosen from* [EACTR-2]].

shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.

7. No subject is allowed to read, write, modify or use the data objects 2b) of FDP_ACF.1.1/TRM.
8. No subject is allowed to read sensitive user data that are protected only by EAC1, except an EAC1 terminal (OID inspection system) after EAC1, cf. FIA_UAU.1/EAC1, that has a corresponding relative authorization level. This includes in particular EAC1-protected user data DG3 and DG4 from an ICAO-compliant ePass application, cf. [EACTR-1] and [ICAO9303].
9. If sensitive user data is protected both by EAC1 and EAC2, no subject is allowed to read those data except EAC1 terminals or EAC2 terminals that access these data according to rule 6 or rule 8 above.
10. Nobody is allowed to read the private signature key(s) [184].

446 *Application Note 66*: The above definition is based on FDP_ACF.1/TRM_EAC2PP. We argue that it covers FDP_ACF.1/TRM_EAC1PP as well. Subject 1 b and 1 d are renamed here from FDP_ACF.1.1/TRM_EAC1PP according to Table 1. Objects in 2), in particular the term EAC1-protected user data, subsume all those explicitly enumerated in FDP_ACF.1.1/TRM_EAC1PP. Also, the security attribute 3 a) Terminal Authorization Level here subsumes the explicitly enumerated attributes 3 a) and 3 b) of FDP_ACF.1.1/TRM_EAC1PP, but are semantically the same. Since in addition EAC2 protected data are stored in the TOE of this PP, additional subjects, objects and security attributes are listed here. However since they apply to data with a different protection mechanism (EAC2), strict conformance is not violated.FDP_ACF.1.2/TRM uses the renaming of Table 1, and references in addition [EACTR-2]. However the references are compatible as justified in [EAC2PP], yet both are mentioned here since [EACTR-2] is the primary norm for an eID application, whereas [ICAOSAC] is normative for an ICAO compliant ePass application. Investigating the references reveals that access to data objects defined in FDP_ACF.1.1/TRM must be granted if these data are neither EAC1-protected, nor EAC2-protected.FDP_ACF.1.3/TRM is the same as in FDP_ACF.1.3/ TRM_EAC2PP.

447 References are changed in FDP_ACF.1.2/TRM_EAC1PP. It is already justified in [EAC2PP] that definitions in [EACTR-2] and [ICAO9303] are compatible.

448 FDP_ACF.1.3/TRM is taken over from [EAC1PP] and [EAC2PP] (same formulation in both).Rules 1 and 2 of FDP_ACF.1.4/TRM_EAC1PP in [EAC1PP] are covered by their counterparts rule 1 and rule 2 here. Rules 3 and 4, and rule 6 of FDP_ACF.1.4/TRM_E\ AC1PP in [EAC1PP] are combined here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of [EAC1PP] is here equivalent to rule 7. None of this conflict with strict conformance to [EAC1PP]. Note that adding additional rules compared to FDP_ACF.1.4/TRM_EAC1PP here can never violate strict conformance, as these are rules that explicitly deny access of subjects to objects. Hence security is always increased. The above definition also covers FDP_ACF.1.1/TRM_EAC2PP and extends it by additional subjects and objects. Sensitive user data in the definition of FDP_ACF.1.1/TRM_EAC2PP are here EAC2-protected sensitive user data. EAC1-protected data are added here by refinement. Since the protection level and mechanisms elated to EAC2-protected data do not change, strict conformance is not violated. FDP_ACF.1.2/TRM_EAC2PP and FDP_ACF.1.3/TRM_EAC2PP are equivalent to the current definition. Rules 8, 9 and 10 are added here by open assignment from [EAC2PP].

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

None of these conflicts with strict conformance. The dependency of this SFR is met by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP. Note that the SFR in [EAC1PP] applies the assignment operation, whereas in [EAC2PP] (by referencing [PACEPP]) the assignment is left open. Hence, they are compatible. We remark that in order to restrict the access to user data as defined in the SFR FDP_ACC.1/TRM_\ EAC1PP, clearly access to objects 2 b) of FDP_ACF.1.1/TRM must be restricted as well according to the SFP, otherwise access to user data is impossible to enforce.

449 **FDP_ACC.1/TRM_EAC2PP Subset access control – Terminal Access**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled

FDP_ACC.1.1/TRM

The TSF shall enforce the Access Control SFP [185] on terminals gaining access to the User Data and data stored in EF.SOD of the electronic document[186].

450 *Application Note 67:* The Protection Profile [PACEPP] allows for extension to cover additional security functionalities. This is not necessary here, as all security functionalities are covered by FDP_ACF.1/TRM.

451 **FDP_RIP.1/EAC2PP Subset residual information protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/EAC2PP

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from*[187] the following objects:

1. Session Keys (**PACE-K_{MAC}, PACE-K_{Enc}**), (**CA-K_{MAC}, CA-K_{Enc}**) ((immediately after closing related communication session)
2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K[188]),
3. secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more),
4. *none*[189].

452 *Application Note 68:* This SFR covers also FDP_RIP.1 from the [EAC1PP] despite this is not explicitly mentioned in [MREDPP].

185 [assignment: *access control SFP*]

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

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

188 according to [EACTR-2]

189 [assignment: *list of objects*]

453 **FDP_UCT.1/TRM_EAC2PP Basic data exchange confidentiality - MRTD**

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
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path] not fulfilled but justified

FDP_UCT.1.1/TRM_EAC2PP

The TSF shall enforce the Access Control SFP[190] to be able to transmit and receive[191] user data in a manner protected from unauthorized disclosure.

454 *Application Note 69*: The SFR FDP_UCT.1 requires the use of secure messaging between the MRTD and the Basic Inspection System. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is also not applicable here.

455 **FDP_UIT.1/TRM_EAC2PP Data Exchange Integrity**

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
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path] not fulfilled but justified

FDP_UIT.1.1/TRM_EAC2PP

The TSF shall enforce the Access Control SFP[192] to be able to transmit and receive[193] user data in a manner protected from modification, deletion, insertion and replay[194] errors.

FDP_UIT.1.2/TRM_EAC2PP

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[195] has occurred.

456 *Application Note 70*: The SFR FDP_UIT.1 requires the use of secure messaging between the MRTD and the Basic Inspection System. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is also not applicable here.

190 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

191 [selection*: transmit, receive*]

192 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

193 [selection*: transmit, receive*]

194 [selection: *modification, deletion, insertion, replay*]

195 [selection: *modification*, *deletion, insertion, replay*]

457 **FDP_ACC.1/UPD Subset access control – Terminal Access**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled

FDP_ACC.1.1/UPD

The TSF shall enforce the Update Access Control SFP [196] on

1. Subjects:
   a. terminal,
   b. update terminal,
2. Objects:
   a. version information identifying the TOE software,
   b. update package
   c. update log information
3. Operations:
   a. reading out version information,
   b. reading out log data,
   c. uploading an update package,
   d. initiating an update procedure.

and *none*[197].

458 **FDP_ACF.1/UPD Security attribute based access control – Terminal Access**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled

FMT_MSA.3 Static attribute initialization: not fulfilled, but justified [MREDONPP]

FDP_ACF.1.1/UPD

The TSF shall enforce the Update Access Control SFP[198] to objects based on the following:

1. Subjects:
   a. terminal,
   b. update terminal,
2. Objects:
   a. version information identifying the TOE software,
   b. update package
   c. update log information
3. Security attributes:
   a. access rights
4. *none* [199].

FDP_ACF.1.2/UPD

196 [assignment: *access control SFP*]

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

198 [assignment: *access control SFP*]

199 [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*]

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

The authentication level of a terminal must be determined by *the PACE protocol*[200] as required by FIA_UAU.1/UPD. Depending on the authentication level, an authenticated update terminal is allowed one or more of the following:

- read one or more data objects from FDP_ACF.1/UPD
- upload an update package to the TOE and initiate the update procedure.

The precise definition of access rights and how the authentication level is calculated from an authenticated terminal is defined in [*TCOSGD*] [201].

FDP_ACF.1.3/UPD

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[202].

FDP_ACF.1.4/UPD

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[203].

459 *Application Note 71*: Note that the write access to the TOE does not imply that the package data will be accepted by the TOE and modifies afterwards the User Data.

460 FDP_IFC.1/UPD Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1/UPD Simple security attributes: fulfilled

FDP_IFC.1.1/UPD

The TSF shall enforce the Update Flow Control SFP[204] on the following:

1. Subjects:
   a. terminal,
   b. update terminal,
2. information:
   a. update package,
   b. update data,
   c. meta-data, such as version information
3. operations:
   a. performing an update[205].

200 [assignment: *list of technical specifications of cryptographic procedures*]

201 [assignment: *list of technical specifications of cryptographic procedures*]

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

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

204 [assignment: *access control SFP*]

205 [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*]

461 FDP_IFF.1/UPD Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1/UPD Simple security attributes: fulfilled
MT_MSA.3 Static attribute initialization: not fulfilled, but **justified**: The update control TSF according to FDP_IFF.1/UPD uses security attributes that have been defined during personalization, and that are 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_IFF.1.1/UPD

The TSF shall enforce the Update Control SFP[206] based on the following types of subject and information security attributes:

1. Subjects:
   a. terminal,
   b. update terminal,
2. information:
   a. update package,
   b. update data,
   c. meta-data, such as version information
3. security attributes:
   a. update package verification status with the values: NOT VERIFIED (default status), SUCCESSFULLY VERIFIED, and VERIFICATION FAILED[207].

FDP_IFF.1.2/UPD

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. The terminal has established a secure channel with the TOE.
2. The TOE shall only accept update packages sent via a secure channel established with an authenticated update terminal[208].

FDP_IFF.1.3/UPD

The TSF shall enforce the following rules in their specific order:

1. The integrity (using the keyed or unkeyed hash function cf. FCS_COP.1/UPD_INT) and authenticity (using the digital signature, cf. FCS_COP.1/UPD_SIG) of the first part of the update package is verified. If the integrity and authenticity are not both validated, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.
2. The first part of the update package is only decrypted, cf. FCS_COP.1/UPD_DEC, if the integrity and authenticity of the that part has been verified in rule 1. If the decryption fails, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.

206 [assignment: *information flow control SFP*]

207 [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*]

208 [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

3. If all parts of the update package have been decrypted, continue with rule 4. Otherwise, apply rules 1. and 2. on the remaining parts (replace 'first part' with 'current part' above) until either all parts have been decrypted, or the procedure has been aborted with VERIFICATION FAILED.
4. If additional meta-data is stored in the update package *as specified in the TCOS update procedure according to* [*TCOSGD*] [209] is not verified as correct according to [*TCOSGD*][210] the security attribute is set to VERIFICATION FAILED and the update package including all associated data are destroyed, cf. FDP_RIP.1. Correctness w.r.t. the referenced technical specification must not contradict any of the given rules here.
5. Next, the TSF shall verify that:
   a. the version number of the update package must be greater than the version of the installed corresponding software package;
   b. the update data are suitable to the specific TOE configuration/platform by checking relevant meta-data (i.e. TOE product identifier, version number etc.).

If all conditions in step 5 are verified, the verification status is set to SUCCESSFULLY VERIFIED. Otherwise abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.

Only if the verification status is SUCCESSFULLY VERIFIED, the TOE shall install the update data[211].

FDP_IFF.1.4/UPD

The TSF shall explicitly authorize an information flow based on the following rules: *none*[212].

FDP_IFF.1.5/UPD

The TSF shall explicitly deny an information flow based on the following rules: *none*[213].

462 **FDP_RIP.1/UPD Subset residual information protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/UPD

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from*[214] the following objects:

1. Session Keys (immediately after closing related communication session)

209 [assignment: *list of meta-data contained in the update package or reference to technical specification(s) defining those*]

210 [assignment: *technical specification(s) defining correct form and content of meta-data*]

211 [assignment: *additional information flow control SFP rules*]

212 [assignment: *rules, based on security attributes, that explicitly authorize information flows*]

213 [assignment: *rules, based on security attributes, that explicitly deny information flows*]

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

2. all ephemeral keys *of the TCOS Update Procedure: K_{auth} , K_{enc}, K_{MAC} (cf.* [*TCOSGD*])[215] related to the update mechanism,
3. Update package, decrypted update data and meta-data uploaded to the TOE or generated during the update procedure,
4. *none*[216].

463 *Application Note 72*: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard. The three ephemeral keys : Kauth, Kenc, KMAC of the TCOS Update Procedure are not accessible later and will be over-written with new key data during the next update.

464 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_SSCDPP	
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	
FDP_ACC.1/SVD_Transfer_SSCDPP	
FDP_ACF.1/SVD_Transfer_SSCDPP	
FDP_ACC.1/Signature-creation_SSCDPP	
FDP_ACF.1/Signature-creation_SSCDPP	
FDP_RIP.1/SSCDPP	FDP_RIP.1 contributes to achievement of OT.Sigy_SigF (eSign-PIN) and OT.SCD_Secrecy (SCD)
FDP_SDI.2/Persistent_SSCDPP	
FDP_SDI.2/DTBS_SSCDPP	

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

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

466 *Application Note 73:* 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 cannot be changed later. The default value of the security attribute

215 [assignment: *listof ephemeral keys or reference to specification*]

216 [assignment: *list of objects*]

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.

467 **FDP_ACC.1/SCD/SVD_Generation_SSCDPP 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_SSCDPP.

FDP_ACC.1.1/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the SCD/SVD Generation SFP[217] on

1. subjects: S.User
2. objects: SCD, SVD
3. operations: generation of SCD/SVD pair[218].

468 **FDP_ACF.1/SCD/SVD_Generation_SSCDPP 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_SSCDPP,
FMT_MSA.3 Static attribute initialization: control: fulfilled by FMT_MSA.3/SSCDPP

FDP_ACF.1.1/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP[219] to objects based on the following: the user S.User is associated with the security attribute “SCD/SVD Management“[220].

FDP_ACF.1.2/SCD/SVD_Generation_SSCDPP

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

S.User with the security attribute “SCD/SVD Management” set to “authorized” is allowed to generate SCD/SVD pair[221].

FDP_ACF.1.3/SCD/SVD_Generation_SSCDPP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[222].

FDP_ACF.1.4/SCD/SVD_Generation_SSCDPP

---

217 [assignment: *access control SFP*]

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

219 [assignment: *access control SFP*]

220 [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*]

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

222 [assignment: *rules, based on security attributes, that explicitly authorize 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[223].

469 **FDP_ACC.1/SVD_Transfer_SSCDPP Subset access control**

Hierarchical to: No other components.

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

FDP_ACC.1.1/SVD_Transfer_SSCD

The TSF shall enforce the SVD_Transfer_SFP[224] on

1. subjects: S.User,
2. objects: SVD,
3. operations: export[225].

470 **FDP_ACF.1/SVD_Transfer_SSCDPP Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACF.1/SVD_Transfer_SSCDPP,
FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCDPP

FDP_ACF.1.1/SVD_Transfer_SSCDPP

The TSF shall enforce the SVD_Transfer_SFP[226] to objects based on the following:

1. the S.User is associated with the security attribute Role,
2. the SVD[227].

FDP_ACF.1.2/SVD_Transfer_SSCDPP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin* [228] is allowed to export SVD[229].

FDP_ACF.1.3/SVD_Transfer_SSCDPP

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

224 [assignment: *access control SFP*]

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

226 [assignment: *access control SFP*]

227 [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*]

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

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

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[230].

FDP_ACF.1.4/SVD_Transfer_SSCDPP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[231].

471 **FDP_ACC.1/Signature_Creation_SSCDPP Subset access control**

Hierarchical to: No other components.

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

FDP_ACC.1.1/Signature-creation_SSCDPP

The TSF shall enforce the Signature-creation_SFP[232] on

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature-creation[233].

472 **FDP_ACF.1/Signature_Creation_SSCDPP Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/Signature_Creation_SSCDPP,

FMT_MSA.3 Static attribute initialization: fulfilled by FMT_MSA.3/SSCD

FDP_ACF.1.1/Signature-creation_SSCDPP

The TSF shall enforce the Signature-creation_SFP[234] 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"[235].

FDP_ACF.1.2/Signature-creation_SSCDPP

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

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

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

232 [assignment: *access control SFP*]

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

234 [assignment: *access control SFP*]

235 [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*]

R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes [236].

FDP_ACF.1.3/Signature-creation_SSCDPP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[237].

FDP_ACF.1.4/Signature-creation_SSCDPP

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”[238].

473 **FDP_SDI.2/Persistent_SSCDPP Stored data integrity monitoring and action**

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1/Persistent_SSCDPP

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[239] on all objects, based on the following attributes: integrity checked stored data[240].

FDP_SDI.2.2/Persistent_SSCDPP

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[241].

474 **FDP_SDI.2/DTBS_SSCDPP Stored data integrity monitoring and action**

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1/DTBS_SSCDPP

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[242] on all objects, based on the following attributes: integrity checked stored DTBS[243].

FDP_SDI.2.2/DTBS_SSCDPP

---

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

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

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

239 [assignment: *integrity errors*]

240 [assignment: *user data attributes*]

241 [assignment: *action to be taken*]

242 [assignment: *integrity errors*]

243 [assignment: *user data attributes*]

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[244].

475 **FDP_RIP.1/SSCDPP Subset residual information protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/SSCDPP

The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[245] the following objects: SCD[246].

476 *Application Note 74:* 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.

6.1.6 Class FMT Security Management

477 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE_EAC1PP, FIA_UID.1/PACE_EAC2PP, FIA_UID.1/EAC2_\Terminal_EAC2PP, see also the Application Note below.

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,
7. EAC2 terminal, if the eID, ePassport and/or eSign application are active,
8. EAC1 terminal, if the ePassort application is active,
9. Electronic document holder[247].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

244 [assignment: *action to be taken*]

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

246 [assignment: *list of objects*]

247 [assignment: *the authorized identified roles*]

478 The following SFRs are defined in [MREDPP]. They concern loading applications onto the IC during manufacturing and relate directly to OT.Cap_Avail_Loader.

479 FMT_LIM.1/Loader Limited Capabilities

Hierarchical to: No other components.

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

FMT_LIM.1.1/Loader

The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying Loader functionality after *TOE Delivery*[248] does not allow stored user data to be disclosed or manipulated by unauthorized users[249]

480 *Application Note 75:* FMT_LIM.1/Loader supplements FMT_LIM.2/Loader allowing for non-overlapping loading of user data and protecting the TSF against misuses of the Loader for attacks against the TSF. The TOE Loader may allow for correction of already loaded user data before the assigned action e.g., before blocking the TOE Loader for TOE Delivery to the end-customer or any intermediate step on the life cycle of the Security IC or the smartcard.

481 FMT_LIM.2/Loader Limited Availability

Hierarchical to: No other components.

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

FMT_LIM.1.2/Loader

The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: The TSF prevents deploying the Loader functionality after *TOE delivery*[250].[251]

482 *Application Note 76:*: The Loader functionality relies on a secure boot loading procedure in a secure environment before TOE delivery to the assigned user and preventing to deploy the Loader of the Security IC after an assigned action, e.g., after blocking the Loader for TOE delivery to the end-user.

483 The following SFRs are imported from [EAC2PP]. They concern mainly applications with EAC2-protected data.

- FMT_MTD.1/CVCA_INI_EAC2PP
- FMT_MTD.1/CVCA_UPD_EAC2PP
- FMT_SMF.1/EAC2PP
- FMT_SMR.1/PACE_EAC2PP This SFR is combined with FMT_SMR.1/PACE_EAC1PP into to by FMT_SMR.1 above.
- FMT_MTD.1/DATE_EAC2PP
- FMT_MTD.1/PA_EAC2PP

248 [assignment: *action*]

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

250 [assignment: *action*]

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

- FMT_MTD.1/SK_PICC_EAC2PP
- FMT_MTD.1/KEY_READ_EAC2PP
- FMT_MTD.1/Initialize_PIN_EAC2PP
- FMT_MTD.1/Change_PIN_EAC2PP
- FMT_MTD.1/Resume_PIN_EAC2PP
- FMT_MTD.1/Unblock_PIN_EAC2PP
- FMT_MTD.1/Activate_PIN_EAC2PP
- FMT_MTD.3/EAC2PP
- FMT_LIM.1/EAC2PP

484 *Application Note 77*: The SFR above concerns the whole TOE, not just applications with EAC2-protected data.

- FMT_LIM.2/EAC2PP

485 *Application Note 78*: The SFRs above concerns the whole TOE, not just applications with EAC2-protected data.

- FMT_MTD.1/INI_ENA_EAC2PP
- FMT_MTD.1/INI_DIS_EAC2PP

486 The following SFRs are imported due to claiming [EAC1PP]. They mainly concern applications with EAC1-protected data.

- FMT_SMF.1/EAC1PP
- FMT_SMR.1/PACE_EAC1PP This SFR is combined with FMT_SMR.1/PACE_EAC2PP into FMT_SMR.1
- FMT_LIM.1/EAC1PP This SFR is equivalent to FMT_LIM.1/EAC2PP, listed here only for the sake of completeness.
- FMT_LIM.2/EAC1PP This SFR is equivalent to FMT_LIM.2/EAC2PP, listed here only for the sake of completeness.
- FMT_MTD.1/INI_ENA_EAC1PP (equivalent to FMT_MTD.1/INI_ENA_EAC2PP, listed here only for the sake of completeness)
- FMT_MTD.1/INI_DIS_EAC1PP (equivalent to FMT_MTD.1/INI_DIS_EAC2PP, listed here only for the sake of completeness)
- FMT_MTD.1/CVCA_INI_EAC1PP
- FMT_MTD.1/CVCA_UPD_EAC1PP (equivalent to FMT_MTD.1/CVCA_UPD_ EAC2PP, listed here only for the sake of completeness)
- FMT_MTD.1/DATE_EAC1PP This SFR is equivalent to FMT_MTD.1/DATE_EAC2PP.

487 Note that FMT_MTD.1/DATE_EAC2PP generalizes the notion of Domestic Extended Inspection System to EAC1 terminals with appropriate authorization level. This does not violate strict conformance to [EAC1PP].

- FMT_MTD.1/CAPK_EAC1PP
- FMT_MTD.1/PA_EAC1PP (equivalent to FMT_MTD.1/PA_ EAC2PP, listed here only for the sake of completeness)
- FMT_MTD.1/KEY_READ_EAC1PP
- FMT_MTD.3/EAC1PP

488 The following SFRs are imported due to claiming [MREDONPP].

- FMT_SMF.1/UPD
- FMT_MTD.1/UPD_SK_PICC
- FMT_MTD.1/UPD_KEY_READ
- FMT_SMR.1/UPD

489 The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the security management of an eSign application.

- FMT_SMR.1/SSCDPP (covered by FMT_SMR.1)
- FMT_SMF.1/SSCDPP
- FMT_MOF.1/SSCDPP
- FMT_MSA.1/Admin_SSCDPP
- FMT_MSA.1/Signatory_SSCDPP
- FMT_MSA.2/SSCDPP
- FMT_MSA.3/SSCDPP
- FMT_MSA.4/SSCDPP
- FMT_MTD.1/Admin_SSCDPP
- FMT_MTD.1/Signatory_SSCDPP

490 **FMT_SMF.1/EAC2PP Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1/EAC2PP

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

1. Initialization,
2. Pre-Personalization,
3. Personalization,
4. Configuration,
5. **Resume and unblock the PIN (if any)**[252],
6. **Activate and deactivate the PIN (if any)**[253].

491 **FMT_SMF.1/EAC1PP Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1/EAC1PP

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

1. Initialization,
2. Personalization,
3. Pre-Personalization,
4. Configuration[254].

492 *Application Note 79*: For the explanation on the role Manufacturer please refer to the Application Note 27; on the role Personalization Agent – to the Application Note 56.

493 *Application Note 80*: 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.

252 unblocking eSign-PIN is managed by FMT_SMF.1/SSCD

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

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

494 **FMT_LIM.1/EAC2PP Limited capabilities**

Hierarchical to: No other components.

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

FMT_LIM.1.1/EAC2PP

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. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed*[255].

495 **FMT_LIM.2/EAC2PP Limited availability**

Hierarchical to: No other components.

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

FMT_LIM.2.1/EAC2PP

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. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed* [256].

496 **FMT_MTD.1/INI_ENA_EAC2PP 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_EAC2PP

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

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

The TSF shall restrict the ability to write[257] the Initialization Data and Pre-personalization Data[258] to the Manufacturer[259].

497 FMT_MTD.1/INI_DIS_EAC2PP 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_EAC2PP

The TSF shall restrict the ability to read out[260] the Initialization Data and the Pre-personalization Data[261] to the Personalization Agent[262].

498 *Application Note 81:* 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 56.

499 FMT_MTD.1/CVCA_INI_EAC2PP 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_EAC2PP

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

258 [assignment: *list of TSF data*]

259 [assignment: *the authorized identified roles*]

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

261 [assignment: *list of TSF data*]

262 [assignment: *the authorized identified roles*]

The TSF shall restrict the ability to write[263] 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-3, A.6.2]
3. initial Current Date
4. *none*[264]

to *the Personalization Agent*[265].

500 *Application Note 82:* The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent in the issuing phase (cf. [EACTR-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-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. [TCOSGD]).

501 **FMT_MTD.1/CVCA_UPD_EAC2PP 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_EAC2PP

The TSF shall restrict the ability to update[266] the

1. Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the Country Verifying Certification Authority Certificate (C_{CVCA}) as required in [EACTR-3, A.6.2]
3. *none*[267]

to Country Verifying Certification Authority[268].

502 *Application Note 83:* 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-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-3, sec. 2.2.3 and 2.2.4]).

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

264 [assignment: *list of TSF data*]

265 [assignment: *the authorized identified roles*]

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

267 [assignment: *list of TSF data*]

268 [assignment: *the authorized identified roles*]

503 **FMT_MTD.1/DATE_EAC2PP 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_EAC2PP

The TSF shall restrict the ability to modify[269] the Current Date[270] to

1. CVCA,
2. Document Verifier,
3. EAC2 terminal (*EIS, ATT or SGT*[271]) possessing an Accurate Terminal Certificate according to [EACTR-3].
4. *none*[272].

504 *Application Note 84:* The authorized roles are identified in their certificates (cf. [EACTR-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-3, A.6.2.3, B.11.1, C.1.3, C.1.5, D.2] for details).

505 **FMT_MTD.1/PA_EAC2PP Management of TSF data – Personalization Agent**

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/PA_EAC2PP

The TSF shall restrict the ability to write[273] the **card/chip security object (SO_C) and** the document Security Object (SO_D)[274] to the Personalization Agent[275].

506 *Application Note 85:* 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 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 56.

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

270 [assignment: *list of TSF data*]

271 [assignment: *list of EAC2 terminal types*]

272 [assignment: *the authorized identified roles*]

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

274 [assignment: *list of TSF data*]

275 [assignment: *the authorized identified roles*]

507 **FMT_MTD.1/SK_PICC_EAC2PP 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_EAC2PP

The TSF shall restrict the ability to *load or create*[276] the Chip Authentication Private Key (SK_{PICC}) and the Restricted Identification Private Key(s)[277] to the Personalization Agent [278].

508 *Application Note* 86: The formulation Chip Authentication Private Key(s) MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{PICC,1}$ and $SK_{PICC,2}$) as well.

509 *Application Note 87:* 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.

510 **FMT_MTD.1/KEY_READ_EAC2PP Management of TSF data – Private Key Read**

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ_EAC2PP

The TSF shall restrict the ability to read[279] the

1. PACE passwords,
2. Personalization Agent Keys,
3. the Chip Authentication private key(s) (SK_{PICC})
4. the Restricted Identification private key(s)
5. *none*[280]

to none[281].

511 **FMT_MTD.1/KEY_READ_EAC1PP Management of TSF data – Private Key Read**

Hierarchical to: No other components.

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

276 [selection: *create, load*]/[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

277 [assignment: *list of TSF data*]

278 [assignment: *the authorized identified roles*]

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

280 [assignment: *list of TSF data*]

281 [assignment: *the authorized identified roles*]

FMT_SMF.1.

FMT_MTD.1.1/KEY_READ_EAC1PP

The TSF shall restrict the ability to read[282] the

1. PACE passwords
2. Chip Authentication Private Key
3. Personalization Agent Keys[283]

to none[284].

512 *Application Note 88:* The formulation Chip Authentication Private Key MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{PICC,1}$ and $SK_{PICC,2}$) as well.

513 **FMT_MTD.1/Resume_PIN_EAC2PP Management of TSF data – Resuming PIN**

Hierarchical to: No other components.

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

FMT_MTD.1.1/Resume_PIN_EAC2PP

The TSF shall restrict the ability to resume[285] the suspended PIN[286] to the electronic document holder[287].

514 *Application Note 89:* Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE *wi*th the PIN. It must be implemented according to [EACTR-2], and is relevant for the status *a*s required by FIA_AFL.1/Suspend_PIN. The electronic document holder is authenticated as required by FIA_UAU.1/PACE using the PIN as the shared password.

515 **FMT_MTD.1/Unblock_PIN_EAC2PP Management of TSF data – Unblocking PIN**

Hierarchical to: No other components.

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

FMT_MTD.1.1/Unblock_PIN_EAC2PP

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

283 [assignment: *list of TSF data*]

284 [assignment: *the authorized identified roles*]

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

286 [assignment: *list of TSF data*]

287 [assignment: *the authorized identified roles*]

The TSF shall restrict the ability to unblock[288] the blocked PIN[289] to

1. the electronic document holder (using the PUK for unblocking),
2. an EAC2 terminal of a type that has the terminal authorization level for PIN management[290].

516 *Application Note 90:* The unblocking procedure must be implemented according to [EACTR-2, 2.5.2] and is relevant for the status as required by FIA_AFL.1/PIN_Blocking. It can be triggered by either (i) the electronic document holder being authenticated as required by FIA_UAU.1/PACE using the PUK as the shared password or (ii) the ATT (FIA_UAU.1/Terminal) proved the Terminal Authorization Level being sufficient for PIN management (FDP_ACF.1/TRM).

517 FMT_MTD.1/Initialize_PIN_EAC2PP Management of TSF data – Activating/Deactivating PIN

Hierarchical to: No other components.

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

FMT_MTD.1.1/Initialize_PIN_EAC2PP

The TSF shall restrict the ability to write[291] the initial PIN and PUK[292] to the Personalization Agent[293].

518 FMT_MTD.1/Activate_PIN_EAC2PP Management of TSF data – Activating/Deactivating PIN

Hierarchical to: No other components.

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

FMT_MTD.1.1/Activate_PIN_EAC2PP

The TSF shall restrict the ability to activate and deactivate[294] the PIN[295] to

An EAC2 terminal of a type that has the terminal authorization level for PIN management[296].

519 *Application Note 91:* The activating/deactivating procedures must be implemented according to [EACTR-2, 2.5.2]. It can be triggered by the ATT (FIA_UAU.1/EAC2_Terminal) that proved a Terminal Authorization Level being sufficient for PIN management (FDP_ACF.1/TRM).

---

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

289 [assignment: *list of TSF data*]

290 [assignment: *the authorized identified roles*]

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

292 [assignment: *list of TSF data*]

293 [assignment: *the authorized identified roles*]

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

295 [assignment: *list of TSF data*]

296 [assignment: *the authorized identified roles*]

520 **FMT_MTD.1/Change_PIN_EAC2PP Management of TSF data – Changing PIN**

Hierarchical to: No other components.

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

FMT_MTD.1.1/Change_PIN_EAC2PP

The TSF shall restrict the ability to change[297] the blocked PIN[298] to[299]

1. *the electronic document holder (using the PUK for unblocking),*
2. *an EAC2 terminal of a type that has the terminal authorization level for PIN management*[300].

521 **FMT_MTD.1/CVCA_INI_EAC1PP 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
FMT_SMR.1 fulfilled

FMT_MTD.1.1/CVCA_INI_EAC1PP

The TSF shall restrict the ability to write[301] the

1. initial Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the initial Country Verifying Certification Authority Certificate (C_{CVCA}), as required in [EACTR, part 3 sec. A.6.2.3]
3. initial Current Date
4. *none*[302]

to *the Personalization Agent*[303].

522 *Application Note 92:* The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent in the issuing phase (cf. [EACTR, part 3 sec. 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 Ter¬minal Authorization Level. Please note that only a subset of the metadata must be stored in the TOE, see [EACTR, sec. A.6.2.3]; storing of further certificate's content is optional. In fact, it is not the initial CVCA Certificate, which is necessary for verification, but the public key included therein, and the self-signature gives no additional security. Therefore, the TOE will expect the initial CVCA Certificate to be written by the Personalization Agent without the self-signature (cf. [TCOSGD]).

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

298 [assignment: *list of TSF data*]

299 [assignment: *the authorized identified roles*]

300 [assignment: *the authorized identified roles that match the list of PIN changing rules conformant to* [EACTR-2]]

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

302 [assignment: *list of TSF data*]

303 [assignment: *the authorized identified roles*]

523 **FMT_MTD.1/CVCA_UPD_EAC1PP Management of TSF data – Country Verifying Certification Authority**

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_UPD_EAC1PP

The TSF shall restrict the ability to update[304] the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[305]

to Country Verifying Certification Authority[306].

524 **FMT_MTD.1/CAPK_EAC1PP Management of TSF data – Chip Authentication Private Key**

Hierarchical to: No other components.

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

FMT_MTD.1.1/CAPK_EAC1PP

The TSF shall restrict the ability to *create or load*[307] the Chip Authentication Private Key[308] to *the Initialization/ Personalization Agent*[309]

525 *Application Note 93:* A Chip Authentication Private Key, which is used in the next step or phase can be created or loaded by the actual user (Initialization or Personalization Agent).

526 **FMT_MTD.3/EAC2PP 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/EAC2PP

The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol 2 and the Terminal Access Control SFP[310].

Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [EACTR-3].

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

305 [assignment: *list of TSF data*]

306 [assignment: *the authorized identified roles*]

307 [selection: *create, load*]

308 [assignment: *list of TSF data*]

309 [assignment: *the authorized identified roles*]

310 [assignment: *list of TSF data*]

527 **FMT_MTD.3/EAC1PP 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/EAC1PP

The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol 1 and the Terminal Access Control SFP[311].

Refinement: The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate.**

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

528 *Application Note 94:* The Terminal Authentication Version 1 is used as required by FIA_UAU.4/PACE_EAC1PP and FIA_UAU.5/PACE_EAC1PP. The Terminal Authorization Level is used as TSF data for access control required by FDP_ACF.1/TRM.

529 This ST includes the SFRs of the SSCD PP [SSCDPP]. These items are applicable, if the eSign application is operational.

SFR identifier	Comments
FMT_SMR.1/SSCDPP	R.Sigy is represented by the electronic document holder, and R.Admin by the Personalization Agent, therefore it is covered by FMT_SMR.1
FMT_SMF.1/SSCDPP	–
FMT_MOF.1/SSCDPP	–
FMT_MSA.1/Admin_SSCDPP	–
FMT_MSA.1/Signatory_SSCDPP	–
FMT_MSA.2/SSCDPP	–
FMT_MSA.3/SSCDPP	–

311 [assignment: *list of TSF data*]

SFR identifier	Comments
FMT_MSA.4/SSCDPP	–
FMT_MTD.1/Admin_SSCDPP	–
FMT_MTD.1/Signatory_SSCDPP	eSign-PIN can be unblocked using the card-global PUK. Although the PP allows using an additional eSign-specific eSign-PUK this is not implemented in the TOE.

530 *Application Note 95:* Note that the iterations /□□□_SSCD from [SSCDPP] are renamed here to /□□□_SSCDPP to avoid a redundant notation like /□□□_SSCD_SSCDPP.

531 FMT_SMF.1/SSCDPP Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1/SSCDPP

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*[312].

532 FMT_MOF.1/SSCDPP Management of security functions behavior

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/SSCDPP.

FMT_MOF.1.1/SSCDPP

The TSF shall restrict the ability to enable[313] the functions signature-creation function[314] to R.Sigy[315].

533 FMT_MSA.1/Admin_SSCDPP 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_SSCD,
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1,

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

313 [selection: *determine the behavior of, disable, enable, modify the behavior of*]

314 [assignment: *list of functions*]

315 [assignment: *the authorized identified roles*]

FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCDPP

FMT_MSA.1.1/Admin_SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP[316] to restrict the ability to modify[317] the security attributes SCD/SVD management[318] to R.Admin[319].

534 *Application Note 96:* The selection[317] is made from a selection with the following assignment: [*selection:* change_default, query, modify, delete, *none*[320]].

535 FMT_MSA.1/Signatory_SSCDPP 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_SSCD
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
FMT_SMF.1 Specification of Management Functions: fulfilled by FMT_SMF.1/SSCDPP

FMT_MSA.1.1/Signatory_SSCDPP

The TSF shall enforce the Signature-creation_SFP[321] to restrict the ability to modify[322] the security attributes SCD operational[323] to R.Sigy[324].

536 FMT_MSA.2/SSCDPP 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_SSCD,
FDP_ACC.1/Signature_Creation_SSCD
FMT_MSA.1 Management of security attributes: fulfilled by FMT_MSA.1/Admin_SSCDPP, FMT_MSA.1/Signatory_SSCDPP
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MSA.2.1/SSCDPP

The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[325].

---

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

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

318 [assignment: *list of security attributes*]

319 [assignment: *the authorized identified roles*]

320 [assignment: *other operations*]

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

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

323 [assignment: *list of security attributes*]

324 [assignment: *the authorized identified roles*]

325 [selection: *list of security attributes*]

537 *Application Note 97:* The security attribute for SCD/SVD Management is 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.

538 FMT_MSA.3/SSCDPP Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes: fulfilled by FMT_MSA.1/Admin_SSCDPP, FMT_MSA.1/Signatory_SSCDPP.
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MSA.3.1/SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-creation_SFP[326] to provide restrictive[327] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SSCDPP

The TSF shall allow the R.Admin[328] to specify alternative initial values to override the default values when an object or information is created.

539 FMT_MSA.4/SSCDPP Security attribute value inheritance

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCD, FDP_ACC.1/Signature_Creation_SSCD

FMT_MSA.4.1/SSCDPP

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[329].

540 *Application Note 98:* Because the TOE does not support SCD/SVD generation by the Signatory alone, the rule (2) is not relevant here.

---

326 [assignment: *access control SFP*, *information flow control SFP*]

327 [selection choose one of: *restrictive, permissive*, [assignment: *other property*]]

328 [assignment: *the authorized identified roles*]

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

541 **FMT_MTD.1/Admin_SSCDPP 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/SSCDPP

FMT_MTD.1.1/Admin_SSCDPP

The TSF shall restrict the ability to create[330] the RAD[331] to R.Admin[332].

542 **FMT_MTD.1/Signatory_SSCDPP 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/SSCDPP

FMT_MTD.1.1/Signatory_SSCDPP

The TSF shall restrict the ability to modify, *unblock*[333] the RAD[334] to R.Sigy[335].

543 *Application Note 99:* The selection[333] is made from a selection with the following assignment: [selection: change_default, query, modify, delete, *unblock*[336]].

544 The following SFRs are imported due to claiming [MREDONPP].

545 **FMT_SMF.1/UPD Specification of Management Functions including Updates**

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/UPD

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

1. Updating the TOE software with the mechanism *TCOS update mechanism* specified in [*TCOSGD*][337]. [338].

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

331 [assignment: *list of TSF data*]

332 [assignment: *the authorized identified roles*]

333 [selection: *change_default, query, modify, delete, clear, create, load,* [assignment: *other operations*]]

334 [assignment: *list of TSF data*]

335 [assignment: *the authorized identified roles*]

336 [assignment: *other operations*]

337 [assignment: *list of technical specification(s) defining an update mechanism*]

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

546 **FMT_MTD.1/UPD_SK_PICC Management of TSF Data – Secret Update Keys**

Hierarchical to: No other components.

Dependencies: FMT_SMR.1: fulfilled
FMT_SMF.1: fulfilled

FMT_MTD.1.1/UPD_SK_PICC

The TSF shall restrict the ability to *create*[339] the *Secret Cryptographic Update Keys*[340] to the update key installation agent.[341].

547 **FMT_MTD.1/UPD_KEY_READ Management of TSF data – Secret Update Keys**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1: fulfilled
FMT_SMR.1: fulfilled

FMT_MTD.1.1/UPD_KEY_READ

The TSF shall restrict the ability to read[342] the

1. *Secret Cryptographic Update Keys*[343]
2. *none*[344]

to none[345].

548 **FMT_SMR.1/UPD Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1: fulfilled

FMT_SMR.1.1/UPD

The TSF shall maintain the roles

1. terminal
2. update terminal
3. update key installation agent
4. *none*[346]

FMT_SMR.1.2/UPD

The TSF shall be able to associate users with roles.

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

340 [selection: *list of, or reference specifying the Secret Cryptographic Update Keys required for the update procedure*]

341 [assignment: *the authorized identified roles*]

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

343 [assignment: *list of or reference specifying the Secret Cryptographic Update Keys required for the update procedure*]

344 [assignment: *list of TSF data*]

345 [assignment: *the authorized identified roles*]

346 [assignment: *list of TSF data*]

6.1.7 Class FPT Protection of the Security Functions

549 The following security functional requirements are imported from [EAC2PP], and address the protection against forced illicit information leakage, including physical manipulation.

- FPT_EMS.1/EAC2PP

550 *Application Note 100*: Note that the PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.

- FPT_FLS.1/EAC2PP
- FPT_TST.1/EAC2PP
- FPT_PHP.3/EAC2PP

551 The following SFRs are imported due to claiming [EAC1PP]. They mostly concern the protection of security functionality related to EAC1-protected data.

- FPT_TST.1/EAC1PP (equivalent to FPT_TST.1/EAC2PP, listed here only for the sake of completeness)
- FPT_FLS.1/EAC1PP (equivalent to FPT_FLS.1/EAC2PP, listed here only for the sake of completeness)
- FPT_PHP.3/EAC1PP (equivalent to FPT_PHP.3/EAC2PP, listed here only for the sake of completeness)
- FPT_EMS.1/EAC1PP

552 The following SFRs are imported due to claiming [MREDONPP].

- FPT_EMS.1/UPD
- FPT_FLS.1/UPD
- FPT_TST.1/UPD

553 The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the protection of security functionality related to eSign application (if available).

- FPT_EMS.1/SSCDPP
- FPT_FLS.1/SSCDPP(subsumed by FPT_FLS.1/EAC2PP)
- FPT_PHP.1/SSCDPP
- FPT_PHP.3/SSCDPP(subsumed by FPT_PHP.3/EAC2PP)
- FPT_TST.1/SSCDPP(subsumed by FPT_TST.1/EAC2PP)

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

555 **FPT_EMS.1/EAC2PP TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/EAC2PP

The TOE shall not emit *power variations, timing variations during command execution*[347] in excess of *non-useful information*[348] enabling access to[349]

1. **the** session keys (PACE-K_{MAC}, PACE-K_{Enc}), **(CA-K_{MAC}, CA-K_{Enc}, both CA2 and CA3)** ,
2. the ephemeral private key ephem-SK_{PICC}-PACE,
3. the Chip Authentication private key (SK_{PICC})**, both CA2 and CA3,**
4. the PIN, PUK,
5. the additional Chip Authentication 3 private sector keys ($SK_{ICC,1}$ and $SK_{ICC,2}$)
6. *none*[350]

and[351]

7. the Restricted Identification private key(s) SK_{ID},
8. *none*[352].

FPT_EMS.1.2/EAC2PP

The TSF shall ensure any users[353] are unable to use the following interface electronic document's contactless/**contact-based interface** and card circuit contacts[354] to gain access to[355]

1. the session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc, both CA2 and CA3),
2. the ephemeral private key ephem - SKPICC- PACE,
3. the Chip Authentication private key (SK_{PICC}), **both CA2 and CA3,**
4. the PIN, PUK,
5. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc}),
6. the additional Chip Authentication 3 private sector keys ($SK_{ICC,1}$ and $SK_{ICC,2}$)
7. *none*[356]

and[357]

8. the Restricted Identification private key(s) SK_{ID},
9. *none*[358].

556 *Application Note 101:* Note that the PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card. The above SFR is refined from [EAC2PP] by adding all relevant key material from Chip Authentication 3 in addition to the key material from Chip Authentication 2, as well as the additional assignment to cover the private sector keys. Thus, the set of keys that need to

347 [assignment: *types of emissions*]

348 [assignment: *specified limits*]

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

350 [assignment: *list of additional types of TSF data*]

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

352 [assignment: *list of additional types of user data*]

353 [assignment: *type of users*]

354 [assignment: *type of connection*]

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

356 [assignment: *list of additional types of TSF data*]

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

358 [assignment: *list of additional types of user data*]

be protected is a superset of the ones of the SFR from [EAC2PP]. Hence, the requirement is stricter than the one from [EAC2PP], and the refinement operation is justified. A refinement is used here to ensure that emissions via contact-based interfaces must not be observable as well. This extends the scope of emission analysis by creating a stricter requirement. Hence, the refinement is justified.

557 **FPT_EMS.1/EAC1PP TOE Emanation – PACE protocol**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/EAC1PP

The TOE shall not emit *power variations, timing variations during command execution*[359] in excess of *non-useful information*[360] enabling access to[361]

1. Chip Authentication **(Version 1)** Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem - SK_{PICC}- PACE,
4. the ephemeral private key $SK_{Map,PICC}$-PACE-CAM
5. *none*[362]
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key,
8. *none*[363].

FPT_EMS.1.2/EAC1PP

The TSF shall ensure any users[364] are unable to use the following interface smart card circuit contacts[365] to gain access to[366]

1. Chip Authentication **(Version 1)** Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem - SK_{PICC}- PACE,
4. the ephemeral private key $SK_{Map,PICC}$-PACE-CAM
5. *none*[367]
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key,
8. *none*[368].

558 *Application Note 102:* This SFR covers the definition of FPT_EMS.1 in [EAC1PP] and extends it by 4. of FPT_EMS.1.1 and FPT_EMS.1.2. Also, 1. and 7. of both FPT_\ EMS.1.1 and FPT_EMS.1.2 are slightly refined in order not to confuse Chip Authentication 1 with

359 [assignment: *types of emissions*]

360 [assignment: *specified limits*]

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

362 [assignment: *list of additional types of TSF data*]

363 [assignment: *list of additional types of user data*]

364 [assignment: *type of users*]

365 [assignment: *type of connection*]

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

367 [assignment: *list of additional types of TSF data*]

368 [assignment: *list of additional types of user data*]

Chip Authentication 2 or Chip Authentication 3. Note that FPT_EMS.1 in [EAC1PP] is solely concerned with Chip Authentication 1, but since it was the first version of the protocol at the time, it was simply called 'Chip Authentication' back then.

559 W.r.t. PACE-CAM, note the significance of protecting $SK_{Map,PICC}$-PACE-CAM. Whereas when running PACE and CA1 separately, gaining knowledge of the ephemeral key SK_{PICC}-PACE enables the attacker to decrypt the current PACE session, an attacker that gains knowledge of the ephemeral key $SK_{Map,PICC}$-PACE-CAM can not only decrypt the session but also easily reveal the static secret chip authentication key SK_{PICC}: Let • denote the group operation (i.e. addition or multiplication), and let i(x) denote the inverse of x. Since the chip sends CA_{PICC} = $SK_{Map,PICC}$-PACE-CAM • i(SK_{PICC}) to the terminal, a malicious attacker that gains knowledge of $SK_{Map,PICC}$-PACE-CAM can reveal SKPICC by computing SK_{PICC} = i(CA_{PICC}) • $SKM_{ap,PICC}$-PACE-CAM.

560 **FPT_EMS.1/UPD TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/UPD

The TOE shall not emit *power variations, timing variations during command execution*[369] in excess of *non-useful information*[370] enabling access to *Secret Update Key*[371] and *any stored user data*[372].

FPT_EMS.1.2/UPD

The TSF shall ensure any users[373] are unable to use the following interface electronic document's contactless/contact-based interface and circuit contacts[374] to gain access to *Secret Update Key* [375] and *any stored user data*[376].

561 *Application Note 103:* The TOE shall prevent 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, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates.

562 **FPT_EMS.1/SSCDPP TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/SSCDPP

369 [assignment: *types of emissions*]

370 [assignment: *specified limits*]

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

372 [assignment: *list of additional types of user data*]

373 [assignment: *type of users*]

374 [assignment: *type of connection*]

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

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

The TOE shall not emit *power variations, timing variations during command execution*[377] in excess of *non-useful information*[378] enabling access to RAD[379] and SCD[380].

FPT_EMS.1.2/SSCDPP

The TSF shall ensure *any users*[381] are unable to use the following interface *the contactless interface and circuit contacts*[382] to gain access to RAD[383] and SCD[384].

563 **FPT_FLS.1/UPD Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/UPD

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

1. Failure during a transmission of the update package data file
2. Failure detected by TSF according to FPT_TST.1
3. Failure detected after a failed update
4. *none*[385].

564 *Application Note 104:* The secure state after a failed update usually reverts to the previous TOE software version. Nevertheless, this capability has limits, since the atomicity of the software update mechanism can technically only be achieved up to a certain extent.

565 **FPT_FLS.1/EAC2PP Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/EAC2PP

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*[386].

377 [assignment: *types of emissions*]

378 [assignment: *specified limits*]

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

380 [assignment: *list of additional types of user data*]

381 [assignment: *type of users*]

382 [assignment: *type of connection*]

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

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

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

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

566 **FPT_PHP.1/SSCDPP Passive detection of physical attack**

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.1.1/SSCDPP

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

FPT_PHP.1.2/SSCDPP

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

567 **FPT_PHP.3/EAC2PP Resistance to physical attack**

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.3.1/EAC2PP

The TSF shall resist physical manipulation and physical probing[387] to the TSF[388] by responding automatically such that the SFRs are always enforced.

568 *Application Note 105*: 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.

569 **FPT_TST.1/EAC2PP TSF Testing**

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1/EAC2PP

The TSF shall run a suite of self tests *during initial start-up*[389] to demonstrate the correct operation of the TSF[390].

FPT_TST.1.2/EAC2PP

The TSF shall provide authorized users with the capability to Verify the integrity of the TSF data[391].

FPT_TST.1.3/EAC2PP

387 [assignment: *physical tampering scenarios*]

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

389 [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*]]

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

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

The TSF shall provide authorized users with the capability to Verify the integrity of stored TSF executable code[392].

570 **FPT_TST.1/UPD TSF Testing**

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1/UPD

The TSF shall run a suite of self tests *during initial start-up*[393] to demonstrate the correct operation of the TSF[394].

FPT_TST.1.2/UPD

The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[395].

FPT_TST.1.3/UPD

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[396].

6.1.8 Class FTP Inter-TSF trusted channel

571 The following SFRs are imported from [EAC2PP].

- FTP_ITC.1/PACE_EAC2PP
- FTP_ITC.1/CA2_EAC2PP[397]

572 The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

- FTP_ITC.1/PACE_EAC1PP

573 The following SFR is imported due to claiming [MREDONPP].

- FTP_ITC.1/UPD

574 **FTP_ITC.1/PACE_EAC2PP Inter-TSF trusted channel after PACE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/PACE_EAC2PP

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **a PACE terminal** that is logically

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

393 [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*]]

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

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

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

397 Note,that in[MREDPP] this SFR is identified as FTP_ITC.1/CA_EAC2PP.

distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **The trusted channel shall be established by performing the PACE protocol according to [EACTR-2].**

FTP_ITC.1.2/PACE_EAC2PP

The TSF shall permit ~~another trusted IT product~~ **a PACE terminal**[398] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC2PP

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE **and a PACE terminal after PACE**[399].

575 *Application Note 106:* 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/PACE_ENC and FCS_COP.1/PACE_MAC.
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/PIN_Blocking.

576 **FTP_ITC.1/CA2_EAC2PP Inter-TSF trusted channel**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/CA2_EAC2PP

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** 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. **The trusted channel shall be established by performing the CA2 protocol according to [EACTR-2].**

FTP_ITC.1.2/CA2_EAC2PP

The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal**[400] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2_EAC2PP

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

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

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

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication[401].

577 *Application Note 107*: Please note that the control on user data stored in the TOE is addressed by FDP_ACF.1/TRM.

578 *Application Note 108:* The requirement FTP_ITC.1/CA2 also covers a secure transport of (i) SVD from the TOE to CGA as well as of (ii) VAD from HID and of (iii) DTBS 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].

579 FTP_ITC.1/CA3 Inter-TSF trusted channel Chip Authentication 3

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/CA3

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** 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. **The trusted channel shall be established by performing the CA3 protocol according to [EACTR-2-v2.20].**

FTP_ITC.1.2/CA3

The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal**[402] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA3

The TSF shall ~~initiate~~**enforce**[403] communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 3.[404].

580 *Application Note 109*: The TOE responds only to commands establishing secure messaging channels.

581 FTP_ITC.1/UPD Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/UPD

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

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

403 **Refinement:** The trusted IT product is the terminal. The word "initiate" is changed to "enforce", because the TOE is a passive device that cannot initiate any communication, but can enforce secured communication if required for an object of the object system and the TOE can close the trusted channel after integrity violation of a received command.

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

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an update terminal** 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/UPD

The TSF shall permit ~~another trusted IT product~~ **an update terminal**[405] to initiate communication via the trusted channel.

FTP_ITC.1.3/UPD

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the update terminal[406].

582 **FTP_ITC.1/PACE_EAC1PP Inter-TSF trusted channel – PACE**

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/PACE_EAC1PP

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PACE_EAC1PP

The TSF shall permit another trusted IT product[407] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC1PP

The TSF shall ~~initiate~~ **enforce**[408] communication via the trusted channel for any data exchange between the TOE and the Terminal[409].

583 *Application Note 110:* The trusted IT product is the terminal. The TOE enforces the trusted channel by means of PACE protocol after establishing a communication channel and reading the ATS.

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

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

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

408 **Refinement:** The trusted IT product is the terminal. The word “initiate” is changed to “enforce”, as the TOE is a passive device that cannot initiate any communication. All communication is initiated by the Terminal, and the TOE enforces the trusted channel.

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

6.2 Security Assurance Requirements for the TOE

584 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).

585 The Protection Profiles BSI-CC-PP0084 [ICPP] and BSI-CC-PP0087 [MREDPP, chap. 6.2.1] define refinements to the TOE Assurance Requirements which are considered by the TOE Developer under the corresponding assurance packages.

6.3 Security Requirements Rationale

586 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the PP ([MREDPP, chap. 6.3.1]) and is therefore not repeated here.

6.3.1 Rationale for SFR's Dependencies

587 The following table provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen. It uses the corresponding Tables from the Protection Profiles ([MREDPP], [MREDONPP], [EAC2PP], [EAC1PP], [PACEPP] and [SSCDPP]). Note that the SFRs and objectives related to the hardware ST are not considered here.

	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OT.Cap_Avail_Loader	OT.Non_Interfere	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE_CAM	OT.AC_Pers_EAC2	OT.CA2	OT.CA3	OT.RI_EAC2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance
FAU_SAS.1/EAC2PP																x				x															
FAU_SAS.1/UPD	x			x																															
FCS_CKM.1/CA_EAC1PP								x	x							x	x	x	x																
FCS_CKM.1/CA3								x					x		x		x	x	x																
FCS_CKM.1/CAM										x							x	x	x																
FCS_CKM.1/UPD_ITC	x	x																																	
FCS_CKM.1/UPD_DEC	x	x																																	
FCS_CKM.1/UPD_INT	x	x																																	
FCS_CKM.1/DH_PACE_EAC1PP																	x	x	x																
FCS_CKM.1/DH_PACE_EAC2PP												x					x	x	x																
FCS_CKM.1/SSCDPP																												x	x	x	x				
FCS_CKM.4/UPD	x	x																																	
FCS_CKM.4/EAC2PP									x								x	x	x																
FCS_CKM.4/SSCDPP																												x	x						
FCS_COP.1/CA_ENC_EAC1PP									x							x																			
FCS_COP.1/CA_MAC_EAC1PP									x							x																			
FCS_COP.1/CAM										x							x	x	x																
FCS_COP.1/UPD_ITC	x	x																																	
FCS_COP.1/UPD_DEC	x	x																																	
FCS_COP.1/UPD_INT	x	x																																	
FCS_COP.1/UPD_SIG	x	x																																	
FCS_COP.1/PACE_ENC_EAC1PP																		x																	

	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OT.Cap_Avail_Loader	OT.Non_Interfere	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE_CAM	OT.AC_Pers_EAC2	OT.CA2	OT.CA3	OT.RI_EAC2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance
FCS_COP.1/PACE_ENC_EAC2PP												x			x			x																		
FCS_COP.1/PACE_MAC_EAC1PP																	x		x																		
FCS_COP.1/PACE_MAC_EAC2PP																	x		x																		
FCS_COP.1/SHA_EAC2PP												x			x		x	x	x																		
FCS_COP.1/SIG_VER_EAC1PP									x							x																					
FCS_COP.1/SIG_VER_EAC2PP															x		x	x	x																		
FCS_COP.1/SSCDPP																												x					x				
FCS_RND.1/EAC2PP									x							x	x	x	X																		
FDP_ACC.1/SCD/SVD_Generation_SSCD																												x				x					
FDP_ACC.1/Signature-creation_SSCDPP																												x						x			
FDP_ACC.1/SVD_Transfer_SSCDPP																												x									
FDP_ACC.1/TRM_EAC2PP											x				x			x	x																		
FDP_ACC.1/UPD	x		x																																		
FDP_ACF.1/UPD	x		x																																		
FDP_ACF.1/SCD/SVD_Genera-																												x				x					
FDP_ACF.1/Signature-creation_SSCDPP																												x						x			
FDP_ACF.1/SVD_Transfer_SSCDPP																												x									
FDP_ACF.1/TRM							x		x						x	x		x	x																		
FDP_IFC.1/UPD	x		x																																		
FDP_IFF.1/UPD	x		x																																		
FDP_RIP.1/UPD	x																																				
FDP_RIP.1/EAC2PP											x	x			x		x	x	x																		
FDP_RIP.1/SSCDPP																													x					x			
FDP_SDI.2/DTBS_SSCDPP																										x								x			
FDP_SDI.2/Persistent_SSCDPP																													x	x			x				
FDP_UCT.1/TRM_EAC2PP											x							x	x																		
FDP_UIT.1/TRM_EAC2PP											x							x	x																		
FIA_AFL.1/Block_PIN_EAC2PP											x				x		x	x	x						x												
FIA_AFL.1/PACE_EAC1PP																																					
FIA_AFL.1/PACE_EAC2PP																									x												
FIA_AFL.1/UPD	x		x																																		
FIA_AFL.1/SSCDPP																																			x		
FIA_AFL.1/Suspend_PIN_EAC2PP											x						x	x	x																		
FIA_API.1/CA_EAC2PP												x			x		x	x	x																		
FIA_API.1/CA3													x	x	x		x	x	x																		
FIA_API.1/EAC1PP								x																													
FIA_API.1/PACE_CAM										x							x	x	x																		
FIA_API.1/RI_EAC2PP														x																							
FIA_UAU.1/EAC2_Terminal_EAC2PP											x				x		x	x	x																		
FIA_UAU.1/PACE_EAC1PP									x							x	x	x	x																		
FIA_UAU.1/PACE_EAC2PP														x			x	x	x																		
FIA_UAU.1/UPD	x		x																																		
FIA_UAU.1/SSCDPP																																	x		x		
FIA_UAU.4/PACE_EAC1PP									x							x	x	x	x																		
FIA_UAU.4/PACE_EAC2PP											x				x		x	x	x																		
FIA_UAU.5/PACE_EAC1PP									x	x							x	x	x																		
FIA_UAU.5/PACE_EAC2PP													x	x	x		x	x	x																		
FIA_UAU.6/CA_EAC2PP															x		x	x	x																		
FIA_UAU.6/CA3													x		x		x	x	x																		
FIA_UAU.6/EAC_EAC1PP															x	x	x	x	x																		
FIA_UAU.6/PACE_EAC2PP																	x	x	x																		
FIA_UID.1/EAC2_Terminal_EAC2PP											x				x		x	x	x																		
FIA_UID.1/PACE_EAC1PP									x	x						x	x	x	x																		
FIA_UID.1/PACE_EAC2PP											x				x		x	x	x																		
FIA_UID.1/UPD	x		x																																		
FIA_UID.1/SSCDPP																																	x		x		
FMT_LIM.1/EAC2PP																						x															
FMT_LIM.1/Loader						x																															
FMT_LIM.2/EAC2PP																						x															
FMT_LIM.2/Loader						x																															
FMT_MOF.1/SSCDPP																												x						x			
FMT_MSA.1/Admin_SSCDPP																												x				x					

	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OT.Cap_Avail_Loader	OT.Non_Interfere	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE_CAM	OT.AC_Pers_EAC2	OT.CA2	OT.CA3	OT.RI_EAC2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance
FMT_MSA.1/Signatory_SSCDPP																												x						x		
FMT_MSA.2/SSCDPP																												x				x		x		
FMT_MSA.3/SSCDPP																												x				x		x		
FMT_MSA.4/SSCDPP																												x		x		x		x		
FMT_MTD.1/UPD_SK_PICC		x	x		x																														
FMT_MTD.1/UPD_KEY_READ		x	x		x																														
FMT_MTD.1/Activate_PIN_EAC2PP											x				x		x	x	x																
FMT_MTD.1/Admin_SSCDPP																												x						x		
FMT_MTD.1/CAPK_EAC1PP								x	x										x																
FMT_MTD.1/Change_PIN_EAC2PP											x				x		x	x	x																
FMT_MTD.1/CVCA_INI_EAC1PP									x																										
FMT_MTD.1/CVCA_INI_EAC2PP															x		x	x	x																
FMT_MTD.1/CVCA_UPD_EAC1PP									x								x	x	x																
FMT_MTD.1/CVCA_UPD_EAC2PP															x		x	x	x																
FMT_MTD.1/DATE_EAC2PP									x						x		x	x	x																
FMT_MTD.1/INI_DIS_EAC2PP															x					x															
FMT_MTD.1/INI_ENA_EAC2PP															x					x															
FMT_MTD.1/Initialize_PIN_EAC2PP															x		x	x	x																
FMT_MTD.1/KEY_READ_EAC1PP								x	x			x					x	x	x																
FMT_MTD.1/KEY_READ_EAC2PP												x			x		x	x	x																
FMT_MTD.1/PA_EAC1PP																x	x	x	x																
FMT_MTD.1/PA_EAC2PP											x	x			x		x	x	x																
FMT_MTD.1/Resume_PIN_EAC2PP											x				x		x	x	x																
FMT_MTD.1/Signatory_SSCDPP																												x						x		
FMT_MTD.1/SK_PICC_EAC2PP												x			x		x	x	x																
FMT_MTD.1/Unblock_PIN_EAC2PP															x		x	x	x																
FMT_MTD.3/EAC1PP									x																										
FMT_MTD.3/EAC2PP															x		x	x	x																
FMT_SMF.1/EAC1PP								x								x	x	x	x	x															
FMT_SMF.1/EAC2PP											x				x		x	x	x	x															
FMT_SMF.1/UPD	x																																		
FMT_SMF.1/SSCDPP																												x		x				x		
FMT_SMR.1		x	x				x	x			x				x	x	x	x	x	x															
FMT_SMR.1/UPD																																			
FPT_EMS.1/EAC1PP							x									x						x													
FPT_EMS.1/EAC2PP							x															x													
FPT_EMS.1/UPD					x																														
FPT_EMS.1/SSCDPP							x																				x		x						
FPT_FLS.1/UPD				x																															
FPT_FLS.1/EAC2PP																				x		x													
FPT_PHP.1/SSCDPP																													x						x
FPT_PHP.3/EAC2PP																			x			x		x											
FPT_TST.1/UPD				x																															
FPT_TST.1/EAC2PP																						x	x					x	x				x		
FTP_ITC.1/CA_EAC2PP															x		x	x	x																
FTP_ITC.1/CA3													x				x	x	x						x										
FTP_ITC.1/UPD	x		x																																
FTP_ITC.1/PACE_EAC1PP																	x	x	x						x										
FTP_ITC.1/PACE_EAC2PP															x		x	x	x						x										

Table 8: SFR coverage

588 The dependency analysis for the security functional requirements given in the corresponding Tables of the Protection Profiles ([MREDPP], [EAC2PP], [EAC1PP], [PACEPP] and [SSCDPP]) shows that the mutual support and internal consistency between all defined functional requirements is satisfied or justified.

6.3.2 Security Assurance Requirements Rationale

589 The assurance package of the Protection Profile was chosen based on the pre-defined assurance package EAL4. This package permits 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 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.

590 The Selection of the component ALC_DVS.2 provides a higher assurance of the security of the travel document's development and manufacturing especially for the secure handling of the travel document's material.

591 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. It is required in the Protection Profile BSI-CC-PP-0084-2014 [ICPP] and is therefore included in this ST.

592 The Selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

593 The set of *assurance* components being part of EAL4 fulfils all dependencies a priori.

594 The component ALC_DVS.2 has no dependencies.

595 The component ATE_DPT.2 has the following dependencies: ADV_ARC.1, ADV_TDS.3 and ADV_FUN.1. All of these are met or exceeded in the EAL4 assurance package.

596 The component AVA_VAN.5 has the following dependencies: ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, and ATE_DPT.1. All of these are met or exceeded in the EAL4 assurance package.

597 Note that the Protection Profile BSI-PP-0087 [MREDPP] refined the Security Assurance Requirements ALC_DEL, ALC_DVS, ALC_CMS, ALC_CMC, ADV_ARC, ADV_FSP, ATE_COV, AGD_OPE, AVA_VAN, ATE_FUN, and ATE_IND. They are all considered for the TOE.

7 TOE Summary Specification

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

599 According to the SFRs the TOE provides the following functionalities, called security services.

- Identification and authentication (SS_HA)
- Secure communication (SS_SM)
- Secure Key Pair Generation (SS_GK)
- Signature Creation (SS_SC)
- Access control for stored objects (SS_AC)
- Update in the field (SS_UiF)
- Reliability of stored information (SS_RE)

600 Almost any security service is supported by some coordinated and matching SFRs. In the following the most important SFRs are associated to security services implemented by the TOE.

7.1 Identification and Authentication

601 The protocols for identification and authentication of users and devices are described in the TCOS Guidance [TCOSGD]. The roles assigned after successful authentication are listed in FMT_SMR.1 and its iterations.

602 The TOE implements asymmetric crypto algorithms used for encryption/decryption, key agreement and digital signatures based elliptic curves. The Selection of the curve used for ECC based algorithm might be a security issue. The TOE supports only the curves defined in [ECCTR] and [FIPS186].

603 The security and the reliability of the identification and authentication are supported by the correct key agreement (FIA_UAU.1, FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6) and the quality of random numbers (FCS_RND.1). This also concerns the authentication via the contactless interface. As soon the authentication state is left, the session keys cannot be used anymore (FCS_CKM.4).

604 The randomness of the parameters of the PACE protocol is guaranteed by the RNG class PTG.3 (FCS_RND.1).

605 User is authenticated with means of PACE passwords, PINs and PUKs, which are bound by corresponding failure or usage counters (FIA_AFL.1). A Terminal is authenticated by using a correct key derived from the provided certificate and the authentication context.

606 Before a user or device is identified only dedicated commands can be executed. This is supported by the iterated SFRs FIA_UID.1.

607 The TOE provides a hybrid physical random number generator of class PTG.3 according to [AIS31] (FCS_RND.1).

608 The TOE implements cryptographic checksum functions, including hash functions used for signature verification and key generation and derivation and message authentication codes (MACs) addressed by FCS_COP.1.

609 Cryptographic functions are necessary for different security protocols implemented by the TOE, e.g. PACE, Chip and Terminal Authentication, or the Update procedure.

610 Cryptographic keys are explicitly deleted by overwriting the memory data with zeros or random numbers, e.g. the new key according to FCS_CKM.4.

611 The SFRs supporting identification and authentication are listed below:

FCS_CKM.1/CA3
FCS_CKM.1/CAM
FCS_CKM.1/DH_PACE_EAC1PP
FCS_CKM.1/DH_PACE_EAC2PP
FCS_CKM.1/CA_EAC1PP
FCS_CKM.4/EAC2PP
FCS_COP.1/CAM
FCS_COP.1/SHA_EAC2PP
FCS_COP.1/SIG_VER_EAC1PP
FCS_COP.1/SIG_VER_EAC2PP
FCS_COP.1/CA3
FCS_RND.1/EAC2PP
FIA_AFL.1/Suspend_PIN_EAC2PP
FIA_API.1/CA_EAC2PP
FIA_API.1/CA3
FIA_API.1/PACE_CAM
FIA_API.1/EAC1PP
FIA_AFL.1/Block_PIN_EAC2PP
FIA_AFL.1/PACE_EAC2PP
FIA_API.1/RI_EAC2PP
FIA_UAU.1/SSCDPP
FIA_UAU.4/PACE_EAC1PP
FIA_UAU.4/PACE_EAC2PP
FIA_UAU.5/PACE_EAC1PP
FIA_UAU.5/PACE_EAC2PP
FIA_UID.1/EAC2_Terminal_EAC2PP
FIA_UID.1/SSCDPP
FIA_AFL.1/SSCDPP
FAU_SAS.1/EAC2PP
FMT_SMR.1
FMT_SMR.1/UPD
FMT_SMF.1/EAC2PP
FMT_SMF.1/EAC1PP
FMT_MTD.1/INI_ENA_EAC2PP
FMT_MTD.1/INI_DIS_EAC2PP
FMT_MTD.1/CVCA_INI_EAC2PP
FMT_MTD.1/CVCA_UPD_EAC2PP
FMT_MTD.1/DATE_EAC2PP

FMT_MTD.1/PA_EAC2PP
FMT_MTD.1/SK_PICC_EAC2PP
FMT_MTD.1/CVCA_INI_EAC1PP
FMT_MTD.1/CVCA_UPD_EAC1PP
FMT_MTD.1/CAPK_EAC1PP
FMT_MTD.3/EAC2PP
FMT_MTD.3/EAC1PP
FMT_MOF.1/SSCDPP
FMT_MTD.1/Signatory_SSCDPP
FMT_MTD.1/UPD_SK_PICC
FDP_RIP.1/EAC2PP

7.2 Secure Communication

612 The secure data exchange in a trusted channel is required by FTP_ITC.1. It is supported by cryptographic operations. The TOE enforces a protected communication over the contactless interface by means of the PACE protocol. It is supported by FDP_UCT.1 and FDP_UIT.1.

613 The strength of algorithms for ensuring confidentiality and integrity is supplied by FCS_COP.1.

614 The TOE provides the symmetric encryption algorithm AES with standardized key lengths of 128, 192 and 256 bits (FCS_COP.1).

615 The SFRs supporting secure communication are listed below:

FCS_COP.1/CA_MAC_EAC1PP
FCS_COP.1/PACE_ENC_EAC1PP
FCS_COP.1/PACE_ENC_EAC2PP
FCS_COP.1/PACE_MAC_EAC1PP
FCS_COP.1/PACE_MAC_EAC2PP
FCS_COP.1/CA_ENC_EAC1PP
FCS_CKM.4/EAC2PP
FDP_UIT.1/TRM_EAC2PP
FTP_ITC.1/CA_EAC2PP
FTP_ITC.1/CA2_EAC2PP
FTP_ITC.1/CA3
FTP_ITC.1/PACE_EAC1PP
FTP_ITC.1/PACE_EAC2PP
FTP_ITC.1/UPD
FIA_API.1/CA_EAC2PP
FIA_API.1/CA3
FIA_API.1/PACE_CAM
FIA_API.1/EAC1PP
FIA_UAU.5/PACE_EAC1PP
FIA_UAU.5/PACE_EAC2PP

FIA_UAU.6/CA_EAC2PP
FIA_UAU.6/CA3
FIA_UAU.6/PACE_EAC2PP
FIA_UAU.6/EAC_EAC1PP
FDP_UCT.1/TRM_EAC2PP
FDP_RIP.1/EAC2PP
FDP_IFF.1/UPD
FDP_RIP.1/UPD
FDP_SDI.2/DTBS_SSCDPP
FMT_SMF.1/SSCDPP

7.3 Secure Key Pair Generation

616 The TOE implements asymmetric crypto algorithms used for secure key pair generation used by signature generation based on elliptic curves. The Selection of the curve used for ECC based algorithm might be a security issue. The TOE supports only the curves defined in [ECCTR] and [FIPS186].

617 The SFRs supporting secure key pair generation are listed below:

FCS_CKM.1/SSCDPP

FCS_CKM.4/SSCDPP

FDP_RIP.1/SSCDPP

FMT_SMF.1/EAC2PP

FMT_SMF.1/EAC1PP

FMT_SMF.1/SSCDPP

FMT_MSA.2/SSCDPP

FMT_MSA.4/SSCDPP

The destruction of the SCD (FCS_CKM.4/SSCDPP) is done on demand of the signatory using the Terminate-command. S.User with the security attribute ‘Role’ set to ‘R.Sigy’ is allowed to destroy the SCD.

7.4 Signature creation

618 The TOE implements asymmetric crypto algorithms for signature generation used for digital signatures based on elliptic curves. The Selection of the curve used for ECC based algorithm might be a security issue. The TOE supports only the curves defined in [ECCTR] and [FIPS186].

619 The SFRs supporting signature creation are listed below:

FCS_COP.1/SSCDPP

7.5 Access Control for stored objects

620 The access to User Data is restricted according to the different iterations of the SFRs FDP_ACC.1 and FDP_ACF.1.

621 According to the SFRs FDP_ACC.1 and FDP_ACF.1 and their iterations the access to User Data is restricted by defined rules laid down in the certified object system. The details can be found in the corresponding SFPs. Note that the TOE enforces these access rules, but there is no a priori protection of a said object. The access rights may be provided by certificates. The TOE can interpret these certificates accordingly.

622 The access to the TOE security functions and the TSF data is controlled by the functionality of the class FMT.

623 The management of the authentication data and corresponding security attributes is implemented according [MREDPP]. The TOE disallows the export of session and authentication keys, passwords and other sensitive user and TSF data. Note that the TOE enforces the access rights of elements of the object system, i.e. data specified as unprotected will be exposed by the TOE. For details refer to the Administrator's Guidance [TCOSGD].

624 The SFRs supporting access control are listed below:

FDP_ACC.1/SCD/SVD_Generation_SSCD
FDP_ACC.1/Signature-creation_SSCDPP
FDP_ACC.1/SVD_Transfer_SSCDPP
FDP_ACC.1/TRM_EAC2PP
FDP_ACC.1/UPD
FDP_ACC.1/SCD/SVD_Generation_SSCDPP
FDP_ACC.1/Signature_Creation_SSCDPP
FDP_ACF.1/SCD/SVD_Generation_SSCDPP
FDP_ACF.1/Signature_Creation_SSCDPP
FDP_ACF.1/SVD_Transfer_SSCDPP
FDP_ACF.1/TRM
FDP_ACF.1/UPD
FDP_IFC.1/UPD
FDP_IFF.1/UPD
FMT_MOF.1/SSCDPP
FIA_AFL.1/Suspend_PIN_EAC2PP
FIA_AFL.1/PACE_EAC2PP
FIA_UID.1/PACE_EAC1PP
FIA_UID.1/PACE_EAC2PP
FIA_UAU.1/PACE_EAC2PP
FIA_UAU.1/EAC2_Terminal_EAC2PP
FIA_UAU.1/PACE_EAC1PP
FIA_UID.1/UPD
FIA_UAU.1/UPD
FMT_SMR.1
FMT_MTD.1/KEY_READ_EAC2PP

FMT_MTD.1/KEY_READ_EAC1PP
FMT_MTD.1/Resume_PIN_EAC2PP
FMT_MTD.1/Unblock_PIN_EAC2PP
FMT_MTD.1/Initialize_PIN_EAC2PP
FMT_MTD.1/Activate_PIN_EAC2PP
FMT_MTD.1/Change_PIN_EAC2PP
FMT_MSA.1/Admin_SSCDPP
FMT_MSA.1/Signatory_SSCDPP
FMT_MSA.3/SSCDPP
FMT_MTD.1/Admin_SSCDPP
FMT_MTD.1/Signatory_SSCDPP
FMT_MTD.1/UPD_KEY_READ

7.6 Update in the Field

625 The TOE supports update in the field, i.e. it is able to make changes to its code in the field (FMT_SMF.1/UPD). According to the SFRs FCS_CKM.1 and FCS_CKM.4 and their iterations the TOE generates and destroys keys required for the secure transport of the update code data.

626 It can store audit records about the update sessions taken place (FAU_SAS.1/UPD).

627 The TOE implements cryptographic checksum functions, including hash functions used for signature verification and key generation and derivation and message authentication codes (MACs) addressed by FCS_COP.1 to secure the update process.

628 Failure handling while the update process is implemented (FIA_AFL.1/UPD) which requires to restart the update procedure on every unsuccessful update attempt.

FAU_SAS.1/UPD
FCS_CKM.1/UPD_DEC
FCS_CKM.1/UPD_INT
FCS_CKM.1/UPD_ITC
FCS_CKM.4/UPD
FCS_COP.1/UPD_DEC
FCS_COP.1/UPD_INT
FCS_COP.1/UPD_ITC
FCS_COP.1/UPD_SIG
FIA_AFL.1/UPD
FDP_IFF.1/UPD
FDP_RIP.1/UPD
FMT_SMF.1/UPD

7.7 Reliability of stored information

629 The operating system of the TOE protects the security functionality of the TOE as soon as it installed during Installation Phase. The TOE will not emit physical or logical data information on security User Data outside the secure channels controlled by the operating system (FPT_EMS.1). User data and TSF data are protected by the TOE if processed or transferred within different parts of the TOE according to the TOE Data Processing Policy of the hardware ST.

630 The TOE will resist physical manipulation and probing and enter a secure state in case a failure occurs. This functionality is supported also by the hardware, which was approved in a separate evaluation process.

631 Dedicated test software is no more available after the TOE is finished (FMT_LIM.1, FMT_LIM.2). These functions are disabled for the TOE in the operational life cycle phase.

632 During TOE manufacturing the chip hardware provides means to store Initialization Data to identify the hardware.

633 Residual information of sensitive data in previously used resources will not be available after its usage (FDP_RIP.1). Session keys and message authentication keys will be destroyed after reset or termination of the secure messaging channel (FCS_CKM.4). The TOE hides the correlation of power or timing variations and the command execution accessing sensitive user data as different keys and passwords (FPT_EMS.1). In case of a malfunction, operating errors or integrity check failures the TOE enters a secure state (FPT_FLS.1). This is supported by the functional services of the hardware.

634 The TOE executes self tests (FPT_TST.1) to demonstrate the correct operation of the TSF and its confidentiality protection capabilities. In case of failures, FPT_FLS.1 requires the preservation of a secure state in order to protect the user data, TSF data and security services.

635 The SFRs supporting protection and the management of User and TSF data are listed below:

FDP_SDI.2/Persistent_SSCDPP
FIA_UID.1/SSCDPP

636 The SFRs supporting self-protection and assurance of the cryptographic functionality are listed below:

FMT_LIM.1/EAC2PP
FMT_LIM.1/Loader
FMT_LIM.2/EAC2PP
FMT_LIM.2/Loader
FPT_EMS.1/EAC1PP
FPT_EMS.1/EAC2PP
FPT_EMS.1/SSCDPP
FPT_EMS.1/UPD
FPT_FLS.1/EAC2PP
FPT_FLS.1/UPD
FPT_PHP.1/SSCDPP
FPT_PHP.3/EAC2PP
FPT_TST.1/EAC2PP

FPT_TST.1/UPD

7.8 Statement of Compatibility

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

7.8.1 Relevance of Hardware TSFs

638 In the following lists the relevance of the hardware security functionality (SF) for the composite security target is considered. All are relevant:

- TSF.Service: Service functionality beside cryptographic operations
- TSF.Protection: General security measures to protect the TSF
- TSF.Control: Operating conditions, memory and hardware access control
- TSF.Crypto: Crypto Service

7.8.2 Security Requirements

Security Functional Requirements

639 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 TOE related to the Composite ST:

640 The Security Requirements of the TOE of the classes FAU, FCS; FIA, FDP, FMT and FTP are specific for the Operating System and have no conflicts with the underlying hardware.

641 The Security Requirements of the TOE of the classes FPT are supported by the Security Functionality TSF.Protection of the hardware ([HWST]) and the AVA_VAN.5 evaluation (FPT_EMS). The requirements FPT_FLS and FPT_PHP are also not conflicting with the requirements for the hardware. They support each other. The requirements for test (FPT_TST) in the operating system are supported by various tests of the hardware (FPT_TST [HW]), and there are no conflicts with the underlying hardware.

Security Requirements of the hardware

642 The Security Requirements of the TOE's hardware based on PP-0084 [ICPP, sec.6.1] and [HWST] can be mapped to Security Requirements of the TOE. They show no conflict between each other.

SFR of the hardware	Relevance	SFR of the TOE using it or meaning
FAU_SAS.1	Re	FAU_SAS.1/EAC2PP
FDP_IFC.1	ReP	concerns information flow policy between parts of the hardware
FDP_SDC.1	ReP	concerns low level stored data protection (confidentiality)

SFR of the hardware	Relevance	SFR of the TOE using it or meaning
FDP_SDI.1	ReP	concerns low level stored data protection (integrity)
FDP_ITT.1	ReP	concerns basic internal transfer protection of the hardware
FMT_LIM.1	Re	FMT_LIM.1 EAC2PP
FMT_LIM.1/Loader	Re	FMT_LIM.1/Loader
FMT_LIM.2	Re	FMT_LIM.2/EAC2PP
FMT_LIM.2/Loader	Re	FMT_LIM.2/Loader
FPT_FLS.1	Re	FPT_FLS.1/EAC2PP, FPT_FLS.1/UPD, FPT_FLS.1/SSCDPP
FRU_FLT.2	Re	
FPT_ITT.1	ReP	concerns basic hardware internal TSF data transfer protection
FPT_PHP.3	Re	FPT_PHP.3/EAC2PP, FPT_PHP.1/SSCDPP
FCS_CKM.1/PUF, FCS_CKM.4/PUF, FCS_COP.1/AES_PUF, FCS_COP.1/MAC_PUF	ReP	concerns internal data protection and therefore does not conflict with key generation in this ST
FPT_TST.1	Re	FPT_TST.1/EAC2PP and FPT_TST.1/UPD
FCS_COP.1/AES	Re	FCS_COP.1/CA_ENC_EAC1PP, FCS_COP.1/CA_MAC_EAC1PP, FCS_COP.1/PACE_ENC_EAC1PP, FCS_COP.1/PACE_ENC_EAC2PP, FCS_COP.1/PACE_MAC_EAC1PP, FCS_COP.1/PACE_MAC_EAC2PP Note that the hardware itself only supports AES in ECB-Mode. The CMAC is implemented by the software using the ECB-Mode of the hardware as base and using the symmetric coprocessor for computing the Xor-operations. The hardware supports Xor-operation of two data-blocks to support chaining-modes which is used here.
FCS_CKM.4/TDES	IR	TDES is not used
FCS_COP.1/TDES	IR	TDES is not used
FCS_RNG.1/PTG.2	Re	FCS_RND.1/EAC2PP
FDP_ACC.1/ACP	Re	FDP_ACC.1 and its iterations of the Composite TOE.
FDP_ACF.1/ACP	Re	FDP_ACF.1 and its iterations
FDP_SDI.2	ReP	concerns low level stored data protection and monitoring and does not conflict with the requirements of this ST

SFR of the hardware	Relevance	SFR of the TOE using it or meaning
FMT_MSA.1/ACP	ReP	concerns the management of security attributes on hardware's level, does not conflict with the SFRs of the TOE
FMT_MSA.3/ACP	ReP	concerns the management of security attributes on hardware's level, does not conflict with the SFRs of the TOE
FMT_SMF.1	ReP	concerns the access of the configuration registers of the Memo¬ry Management Unit, does not conflict with the SFRs of the TOE
FCS_CKM.4/AES	ReP	concerns the internal destruction of the key in the AES coprocessor. It does not conflict with the SFRs of the TOE.
FPT_PHP.3	Re	FPT_PHP.3/EAC2PP and FPT_PHP.1/SSCDPP
FTP_ITC.1/Loader FDP_UCT.1/Loader, FDP_UIT.1/Loader, FDP_ACC.1/Loader, FDP_ACF.1/Loader	IR	Not relevant because the Loader is blocked after TOE delivery
FCS_COP.1/TDES_LIB, FCS_COP.1/AES_LIB, FCS_CKM.4/TDES_LIB, FCS_CKM.4/AES_LIB, FCS_RNG.1/DRG.4 FCS_RNG.1/PTG.3, FCS_COP.1/RSA, FCS_CKM.5/ RSA_PubkeyDerivation, FCS_CKM.1/ RSA_KeyGen, FCS_CKM.4/RSA, FCS_COP.1/ECDSA, FCS_COP.1/ECC_DHKE, FCS_CKM.1/ ECC_KeyGen, FCS_CKM.4/ECC, FCS_COP.1/SHA	IR	All SFRs from the hardware ST related to the crypto library of the hardware are not mapped because the library is not used in the presented TOE.

IR means: **Ir**relevant Platform-SFRs not being used by the Composite-ST.

Re means: **Re**levant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.

ReP means: **Re**levant Platform-SFRs being used by the Composite-ST because of its security properties providing **p**rotection against attacks to the TOE as a whole.

Security Assurance Requirements

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

644 The chosen level of assurance of the hardware is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2. This includes ALC_DVS.2, ATE_DPT.3 and AVA_VAN.5.

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

7.8.3 Security Objectives

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

647 The following Security Objectives of the TOE are related to the Composite ST and are not relevant for the hardware:

- OT.Non_Interfere
- OT.Chip_Auth_Proof
- OT.Sens_Data_Conf
- OT.Chip_Auth_Proof_PACE_CAM
- OT.AC_Pers_EAC2
- OT.CA2
- OT.CA3
- OT.RI_EAC2
- OT.Sens_Data_EAC2
- OT.AC_Pers
- OT.Data_Authenticity
- OT.Data_Confidentiality
- OT.Data_Integrity
- OT.Identification
- OT.Tracing
- OT.DTBS_Integrity_TOE
- OT.SCD_Secrecy
- OT.SCD_SVD_Corresp
- OT.SCD_Unique
- OT.SCD/SVD_Auth_Gen
- OT.Sig_Secure
- OT.Sigy_SigF
- OT.Tamper_ID
- OT.Update_MechanismTOE
- OT.Enc_Sign_Update
- OT.Update_Terminal_Auth
- OT.Attack_Detection
- OT.Key_Secrecy
- OT.Lifecycle_Security

648 The following Security Objectives of the [composite] TOE are (partially) covered by objectives of the hardware [platform]

- O.Leak-Forced and O.Leak-Inherent contribute to OT.Prot_Inf_Leak
- O.Phys-Probing contributes to OT.Prot_Phys-Tamper

- O.Malfunction contributes to OT.Prot_Malfunction
- O.Phys-Manipulation contributes to OT.Prot_Phys-Tamper
- O.Abuse-Func contributes to OT.Prot_Abuse-Func
- O.Identification contributes to OT.Identification
- O.RND, O.AES contributes to OT.Data_Authenticity, OT.Data_Confidentiality, OT.Data_Integrity for the TOE using this hardware functionality
- O.Leak-Forced and O.Leak-Inherent contribute to OT.EMSEC_Design
- O.Leak-Forced and O.Leak-Inherent contribute to OT.Tamper_Resistance
- O.Cap_Avail_Loader and O.Ctrl_Auth_Loader contribute to OT.Cap_Avail_Loader

649 The objective O.TDES is not relevant because the TOE does not use TDES.

650 The remaining objectives of the hardware concern the internal processing of the hardware and are not related to specific objectives of the TOE. They do not conflict to each other:

- O.NVM-Integrity
- O.Access-Control
- O.Self-Test
- O.PUF
- O.RSA, O.ECC both not relevant as the crypto library of the hardware is not used

651 The Security Objectives for the Environment of the TOE are related to the life cycle phase “Operational Use” and do not conflict with the Security Objectives for the hardware which are related to the manufacturing process. Therefore, they do not conflict to each other.

652 Security Objective for the environment of TOE’s hardware:

- OE.Resp-Appl
- OE.Process-Sec-IC
- OE.Lim_Block_Loader
- OE.Loader_Usage
- OE.Check-Init

653 Security Objective for the environment of composite TOE:

- OE.Lim_Block_Loader
- OE.Auth_Key_Travel_Document
- OE.Authoriz_Sens_Data
- OE.Exam_Travel_Document
- OE.Ext_Insp_Systems
- OE.Ext_Insp_Systems
- OE.Chip_Auth_Key
- OE.RestrictedIdentity
- OE.Terminal_Authentication
- OE.Legislative_Compliance
- OE.Passive_Auth_Sign
- OE.Personalization
- OE.Terminal
- OE.Travel_Document_Holder
- OE.CGA_QCert
- OE.DTBS_Intend
- OE.DTBS_Protect
- OE.HID_VAD

- OE.Signatory
- OE.SSCD_Prov_Service
- OE.SVD_Auth
- OE.Code_Confidentiallity
- OE.Secure_Environment
- OE.Eligible_Terminals_Only

7.8.4 Conclusion

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

7.9 Assurance Measures

655 The documentation is produced compliant to the Common Criteria Version 3.1. The following documents provide the necessary information to fulfill the assurance requirements listed in section 6.2 Security Assurance Requirements for the TOE.

Development
- ADV_ARC.1 Security Architecture Description TCOS ID 2.0 Release 1
- ADV_FSP.4 Functional Specification TCOS ID 2.0 Release 1
- ADV_IMP.1 Implementation of the TSF TCOS ID 2.0 Release 1
- ADV_TDS.3 Modular Design of TCOS ID 2.0 Release 1

Guidance documents
- AGD_OPE.1 User Guidance TCOS ID 2.0 Release 1
- AGD_PRE.1 Administrator Guidance TCOS ID 2.0 Release 1

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 ID 2.0 Release 1
- ALC_TAT.1, ALC_DVS.2 Development Tools and Development Security for TCOS ID 2.0 Release 1

Tests
- ATE_COV.2, ATE_DPT.2 Test Documentation for TCOS ID 2.0 Release 1
- ATE_FUN.1 Test Documentation of the Functional Testing

Vulnerability assessment
- AVA_VAN.5 Independent Vulnerability Analysis TCOS ID 2.0 Release 1

656 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.

657 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 installation, personalization and start-up of the TOE.

658 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.

659 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.

660 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 Deutsche Telekom Security GmbH.

661 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

662 The terminology and abbreviations of Common Criteria version 3.1 [CC], Revision 5 apply to this ST. The following table is taken over from the PP [MREDPP]

Acronyms

Acronym	Term
CAP	Composed Assurance Package
CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
OS	Operating System
OSP	Organizational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation

References

[AIS31]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 3.0, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 5 vom 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ANSX9.63]

American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2005-11

[ALGO]

ETSI Technical Specification TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites; European Telecommunication Standards Institute (ETSI), version 1.2.1 or later, 2017-0511

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,

Part 1: Introduction and general model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security functional components; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security assurance components; Version 3.1, April 2017, CCMB-2017-04-003

Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, April 2017, CCMB-2017-04-004

[EACTR]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Bundesamt für Sicherheit in der Informationstechnik (BSI),

Part 1 – eMRTDs with BAC/PACEv2 and EACv1, version 2.20, 2015-02

Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS), version 2.21, 2016-12

Part 3 – Common Specifications, version 2.21, 2016-12

Part 4 – Applications and Document Profiles, version 2.21, 2016-12

[BACPP]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0055-2009, 2009-03

[EAC1PP]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control with PACE (EAC PP) Version 1.3.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0056-V2-2012-MA02, 2012-12

[EAC2PP]

CC Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 Version 1.01, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0086-2015, 2015-05

[ECCTR]

Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018-06-01

[eIDAS]

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the EU, 2014 L 257/73, 2014-08-28

Commission Implementing Decision (EU) 2016/650 of 25 April 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal 2016 of the EU, L 109/40, 2016-04-26

[FIPS180]

Federal Information Processing Standards Publication FIPS PUB 180-4, Secure Hash Standard (SHS), 2015-08

[FIPS186]

Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[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-1149-2022 for NXP Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1) From NXP Semiconductors Germany GmbH
and
Assurance Continuity Maintenance Report, BSI-DSZ-CC-1149-2022-MA-01 NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors

[HWST]

NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1), Security Target Lite Rev. 1.4 — 14 October 2022, Evaluation document BSI-DSZ-CC-1149-MA-01

[ICAOSAC]

ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, ICAO, 2010-11

[ICAO9303]

ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021

[ISO7816]

ISO 7816-4:2013, Identification cards – Integrated circuit cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2013-04

[ISO14443]

ISO 14443, Identification cards – Contactless integrated circuit cards – Proximity cards, Parts 1-4 and Amendments, 2008-2014

[MREDPP]

CC Protection Profile Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], Version 2.03, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0087-V2-2016-MA-01, 2016-07

[MREDONPP]

CC Protection Profile Machine-Readable Electronic Documents – Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], Version 0.9.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0090-2016, 2016-08

[PACEPP]

CC Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.01, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0068-V2-2011-MA01, 2014-07

[ICPP]

Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0084-2014, 2014-01

[RFC5639]

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

[SP800-38A]

Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, December 2001

[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 419211-2:2013, CEN/ISSS, Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0059-2009-MA-02, 2016-06

[TCOSGD]

Guidance TCOS ID Version 3.0 Release 1/P71, Deutsche Telekom Security GmbH, Version 1.0, 2023-03

[TR02102]

Technische Richtlinie TR-02102-1 Kryptographische Verfahren Empfehlungen und Schlüssellängen, Version 2023-01, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023-01-09