Federal Office
for Information Security

Common Criteria Protection Profile

Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP]

BSI-CC-PP-0087-V2

Version 2.0.2

Document history

Version 2.0.2, April 4th, 2016

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Figures

Tables

1 PP Introduction

This section provides document management and overview information required to register the protection profile and to enable a potential user of the PP to determine, whether the PP is of interest.

1.1 PP Reference

Title:	Common Criteria Protection Profile 'Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP]'
Editor/Sponsor:	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI))
CC Version:	3.1 (Revision 4)
Assurance Level:	Minimum assurance level for this PP is EAL4 augmented.
General Status:	final
Version Number:	Version 2.0.2 as of April 4th, 2016
Registration:	BSI-CC-PP-0087-V2
Keywords:	ICAO, PACE, EAC, Extended Access Control, ID-Card, electronic document, smart card, TR-03110

1.2 TOE Overview

This PP claims strict conformance to [PACEPP], [EAC1PP] and [EAC2PP]. There, slightly different terminology is used. For the ease of understanding, Table 1 gives a brief translation for the used terminology. Compound words that contain terminology of the table should be replaced accordingly.

This PP	PACE PP	EAC1PP	EAC2PP
electronic document	travel document	travel document	electronic document
electronic document presenter	traveler	traveller	electronic document presenter
EAC1 protected data	-	sensitive (user) data	-
EAC2 protected data	-	-	sensitive user data
common user data	user data	user data	common user data
PACE terminal	BIS-PACE	BIS-PACE	PACE terminal
EAC1 terminal	-	Extended Inspection System	-
EAC2 terminal	-	-	EAC2 terminal

Table 1: Overview of identifiers of this and claimed PPs.

1.2.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) is a smartcard programmed according to [TR03110-1] and [TR03110-2]. The smartcard contains multiple applications (at least one). The programmed smartcard is called an electronic document as a whole. Here, an application is a collection of 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:

1. *EAC1-protected data:* Sensitive user data protected by EAC1 (cf. [TR03110-1]),
2. *EAC2-protected data:* Sensitive user data protected by EAC2 (cf. [TR03110-2]), and
3. *all other (common) user data*. Other user data are protected by Password Authenticated Connection Establishment (PACE, cf. also [TR03110-2]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE.

Application Note 1: Due to migration periods, some developers have to implement products that functionally support both PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC) [ICAO9303]. However, any product using BAC is not conformant to the current PP; i.e. the TOE may functionally support BAC, but, while performing BAC, it is acting outside of the security policy defined by the current PP.

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

Applications considered in [TR03110-1] and [TR03110-2] are

1. an electronic passport (ePass) application (containing common and EAC1 protected data, and being conformant to [ICAO9303]),
2. an electronic identity (eID) application (containing common and EAC2 protected data), and
3. a signature (eSign) application (protected by EAC2).

A *configuration of the TOE* is a combination of one or several of the above applications together with corresponding common data, sensitive data, and TSF data. This protection profile however does not make any assumptions on what kind of applications, and how many applications are included. Chapter 1.3 provides guidance on how this protection profile is intended to be used for product development and certification, and Chapter 1.2.6 gives recommendations for a TOE design w.r.t. applications and data groups.

The combination of different applications for a product corresponds to loading different data into the EEPROM or flash memory of a smart card. Such a configuration of data groups yields a specific electronic document.

Applications, that is configurations of data groups, are loaded during manufacturing. Requirements on the loader are adapted from the *CC-Package: Package 1: Loader dedicated for usage in secured environment only* from [ICPP]. If needed, additional requirements should be defined by the ST-writer.

As mentioned, access to common and sensitive user data is protected by PACE, EAC1, and/or EAC2 (see below). Thus the electronic document holder can control access to her user data either by consciously presenting her electronic document, and/or by consciously entering a secret personal identification number (PIN).

A data group should be defined by the ST-Writer as either sensitive user data protected by EAC1, sensitive user data protected by EAC2, or common user data. Obviously, if a data group is for example defined as sensitive user data protected by EAC1, but is at the same time defined as common user data and thus accessible by just PACE alone, this defeats the whole purpose of protecting it with the advanced security mechanism EAC1 in the first place. However, to ensure compatibility with standards set by the International Civil Aviation Organization (ICAO) for electronic passports, exceptions are acceptable for certain applications. See also Chapter 1.2.6 for details.

The TOE shall comprise at least

1. the circuitry of the chip, including all integrated circuit (IC) dedicated software that is active in the operational phase of the TOE,
2. the IC embedded software, i.e. the operating system,
3. all access mechanisms, associated protocols and corresponding data,

4. one or several applications, and
5. the associated guidance documentation.

Application Note 2: Since contactless interface parts (e.g. the antenna) may impact specific aspects of vulnerability assessment and are thus relevant for security, such parts might be considered as a part of the TOE. The decision upon this is up to the certification body in charge that defines the evaluation methodology for the assessment of the contactless interface.

1.2.2 TOE major Security Features for Operational Use

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, if the TOE contains an eSign application.

1.2.3 TOE Type

The TOE type addressed by the current protection profile is a smartcard programmed according to [TR03110-1] and [TR03110-2]. The smartcard contains multiple applications (at least one). The programmed smartcard is called an electronic document as a whole.

Justification: TOE type definitions of the claimed PPs ([EAC1PP], [EAC2PP], [SSCDPP]) differ slightly. We argue that these differences do not violate consistency:

The TOE type defined both in [EAC1PP] and [EAC2PP] is a smartcard. Whereas [EAC1PP] references [TR03110-1] (and also [ICAO9303] and related ICAO specifications, however [TR03110-1] is fully compatible with those ICAO specifications, and they are mostly listed there for the sake of completeness and the context of use) w.r.t. programming of the card, [TR03110-2] is given as a reference in [EAC2PP]. Reference [TR03110-1] defines the EAC1 protocol, whereas EAC2 is defined in [TR03110-2]. Thus this difference in reference is introduced just due to different applications on the card, that do not contradict each other. The term 'travel document' of [EAC1PP] is here understood in a more broader sense (cf. also Table 1), since the document can also be used in contexts other than just traveling.

Moreover, [TR03110-2-v2.20] is referenced in difference to the claimed PPs. This reference is only needed for the specification of Chip Authentication 3, an upgraded and extended version of Chip Authentication 2. Since the TOE also supports Chip Authentication 2 there is full compatibility; consistency is not violated.

The TOE type definition given in [SSCDPP] is "*a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD)*". The definition of hardware and software in this PP is more specific by explicitly mentioning a smartcard and the software on the card. However the very fundamental purpose of a smartcard is to store data on it in a protected way. Hence, the TOE type definition of this PP is also not inconsistent with the one of [SSCDPP].

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 installation of the smart card applications and their electronic
110 personalization, i. e. tying the application data up to the electronic document holder.

Operational use of the TOE is explicitly in the focus of current PP. Nevertheless, some TOE functionality might not be directly accessible to the end-user during operational use. Some single properties of the manufacturing and the card issuing life cycle phases that are significant for the security of the TOE in its operational phase are also considered by the current PP. Conformance with this PP requires that all life cycle
115 phases are considered to the extent that is required by the assurance package chosen here for the TOE; c.f. also Chapter 6.2.

1.2.4 TOE Life Cycle

The TOE life cycle is described in terms of the above mentioned four life cycle phases. Akin to [ICPP], the TOE life-cycle is additionally subdivided into seven steps.

Phase 1: Development

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

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.

125 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.

Phase 2: Manufacturing

Step 3
In a first step, the TOE integrated circuit is produced. The circuit contains the electronic document's chip
130 dedicated software, and the parts of the electronic document's chip embedded software in the non-volatile non-programmable memory (ROM). 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. If necessary, the IC manufacturer adds parts of the
135 IC embedded software in the non-volatile programmable memory, e. g. EEPROM.

Step 4 (optional)
If the electronic document manufacturer delivers a packaged component, the IC is combined with hardware for the contact based or contactless interface.

Step 5
The electronic document manufacturer

1. if necessary, adds the IC embedded software, or parts of it in the non-volatile programmable
140 memories, e. g. EEPROM or FLASH,
2. creates the application(s), and
3. equips the electronic document's chip with pre-personalization data.

Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), and elementary files (EFs) according to [ISO7816-4]. How this process is handled internally depends on the IC and
145 IC embedded software.

The pre-personalized electronic document together with the IC identifier is securely delivered from the electronic document manufacturer to the personalization agent. The electronic document manufacturer also provides the relevant parts of the guidance documentation to the personalization agent.

Phase 3: Personalization of the Electronic Document

Step 6
The personalization of the electronic document includes

150 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.

155 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.

160 *Application Note 3*: TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies [CC1]. Here TSF data include, but are not limited to, the personalization agent's authentication key(s).

Phase 4: Operational Use

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.

165 *Application Note 4*: This PP considers at least the first phase and parts of the second phase, i.e. Step 1 up to Step 3, as part of the evaluation. Therefore the TOE delivery is defined to occur, according to CC, after Step 3. Since specific production steps of the second phase are of minor security relevance (e.g. plastic card or booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national
170 body of the issuer or organization. In this case the national body of the issuer is responsible for these specific production steps.
Note that the personalization process and its environment may depend on specific security needs of the issuer. All production, generation and installation procedures after TOE delivery up to the phase *operational use* have to be considered in the product evaluation process under assurance class AGD. Therefore,
175 the security target has to outline how to split up P.Manufact, P.Personalisation and related security objectives into aspects relevant before vs. those relevant after TOE delivery.

Some production steps, e. g. Step 4 in Phase 2 may also take place in the Phase 3.

1.2.5 Non-TOE Hardware/Software/Firmware

In order to be powered up and to communicate with the external world, the TOE needs a terminal (card reader) supporting the communication according to [ISO7816-4] and [ISO14443]; the latter only if the card
180 has a contactless interface. Akin to [TR03110-1] and [TR03110-2] the TOE shall be able to recognize the following terminal types:

– **PACE terminal**. A PACE terminal is a basic inspection system according to [TR03110-1], [TR03110-2] resp. It performs the standard inspection procedure, i.e PACE followed by Passive Authentication, cf. [TR03110-1]. 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 ePass application)**. An EAC1 terminal is an extended inspection system according to [TR03110-1]. It performs the advanced inspection procedure ([TR03110-1]) 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 [TR03110-2] 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.

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 [TR03110-3]. For the access rights, cf. also the SFR component FDP_ACF.1/TRM in Chapter 6.1.3.

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 [TR03110-3].

The term *terminal* within this PP usually refers to any kind of terminal, if not explicitly mentioned otherwise. If this PP is claimed for a security target, the ST-Writer shall give an overview of which of the above terminals are related to what application, and which data group is accessible. Chapter 1.2.6 must be taken into account.

Other terminals than the above are out of scope of this PP. In particular, terminals using Basic Access Control (BAC) may be functionally supported by the electronic document, but if the TOE is operated using BAC, it is not in a certified mode.

1.2.6 Recommended TOE Design

The electronic document may contain one of the following combinations of applications and protocols:

- *Passport configuration*: user data stored in an ICAO-compliant ePass application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.
- *Residence permit configuration*: user data stored in an ICAO-compliant ePass application protected by PACE and EAC1/EAC2. Additional user data are stored in [TR03110-2] conformant eID and eSign applications, and are protected by EAC2.
- *Electronic Document configuration*: user data contained in [TR03110-2]-conformant eID, and eSign applications. An ePass application is included as well, but not compliant to [ICAO9303], since user data of all applications are protected by PACE/EAC2.

The purpose and usage of the above mentioned different applications is as follows:

- An **ePass application**, as defined in [ICAO9303], is intended to be used by authorities as a machine readable travel document (MRTD). For the ePassport application, the electronic document holder can control access to his user data by consciously presenting his electronic document to authorities[1].

1 CAN or MRZ user authentication, see [TR03110-1]

- An **eID application**, as defined in [TR03110-2], including related user data and data needed for authentication, is intended to be used for accessing official and commercial services which require access to user data stored in the application. For an eID application, the electronic document holder can control access to his user data by inputting his secret PIN (eID-PIN) or by consciously presenting his electronic document to authorities[2];
- An **eSign application**, as defined in [TR03110-2], is intended to generate qualified electronic signatures. The main specific property distinguishing qualified electronic signatures from other, i.e. advanced electronic signatures, is that they are based on qualified certificates and created by secure signature creation devices (SSCD). An eSign application, if implemented, can optionally be activated on the electronic document by a Certification Service Provider, or on his behalf. For an eSign application, the electronic document holder can control access to the digital signature functionality by consciously presenting his electronic document to an EAC2 terminal and inputting his secret PIN (eSign-PIN) for this application[3].

Each application contains its own set of user data, composed according to its requirements.

Application note 5: While it is technically possible to grant access to the electronic signature functionality by inputting only the CAN (see [TR03110-2]), this technical option shall not be allowed by the security policy defined for the eSign application; see the related conformance claim in section 2.2. This is due to the fact that solely the signatory – which is here the electronic document holder – shall be able to generate an electronic signature on his own behalf.

Application note 6: Requiring the document holder to use a separate eSign-PIN to generate qualified signatures represents a manifestation of his declaration of intent bound to this secret PIN. In order to reflect this fact, it should be considered to provide the eID and the eSign applications with organizationally different values of the respective secret PINs (eID-PIN and eSign-PIN). This is especially important, if the eSign application is intended to generate qualified electronic signatures.

1.3 Guidance for using this Protection Profile

1.3.1 Motivation

Electronic document manufacturers often create multiple documents for different purposes. Examples are electronic identity cards, electronic passports, or electronic residence permits. If one protection profile for each electronic document exists, several evaluations are required. Due to that, one chip that has been certified to be used for example for an electronic residence permit, cannot be used for an electronic passport. This is even though the security and functional mechanisms in an electronic residence permit card are a superset of those in an electronic passport. This protection profile intends to address that problem. It is on top of a hierarchy of claimed protection profiles, and thus all potentially required security functionality and mechanisms are included.

2 eID-PIN or CAN user authentication, see [TR03110-2]
3 CAN and eSign-PIN user authentication, see [TR03110-2]

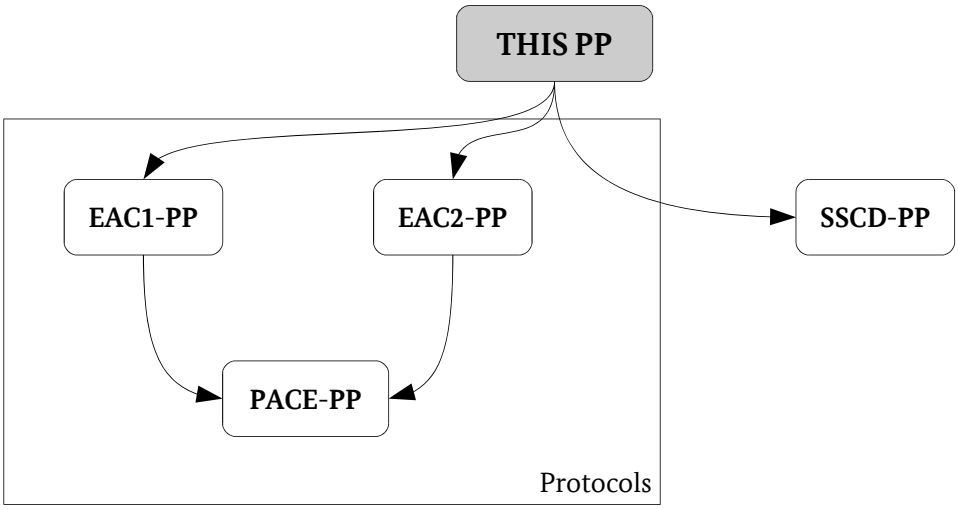

Figure 1: Claims of this PP. A claim is represented by a directed arrow.

1.3.2 Usage

The intended usage is that the manufacturer during the development phase and/or at the beginning of the manufacturing phase (*Step 3)* develops an IC-chip with integrated software that includes all security functionality and mechanisms described within this PP. However prior to personalization (i.e. *Step 5* during manufacturing), only those applications (datagroups) required for the intended final document and their access rights are created. Creation of the applications (i.e. the ISO7816-4 conforming file structure) including datagroups and their access rights) is subject to a limited availability and limited capability policy defined in the family FMT_LIM. In particular, the loader must ensure that creation or alteration of the filesystem is not possible after the manufacturing phase (this excludes populating datagroups with values, as is done in the personalization phase). In summary, this allows *manufacturers* to use a *single* IC for *all* kinds of electronic documents.

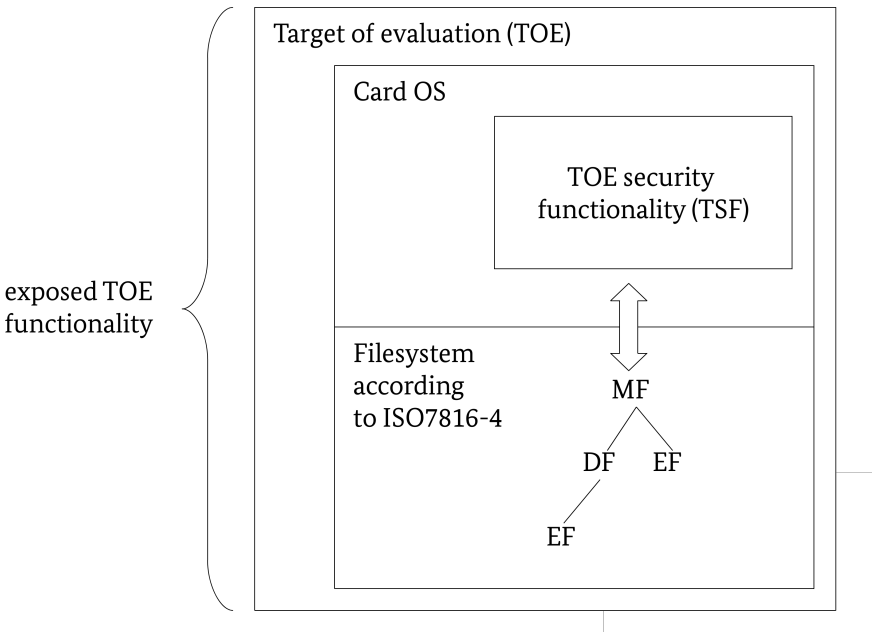

Figure 2: Overview of TOE and TSF

1.3.3 TOE Functionality versus TSF

An abstract description of the TOE is depicted in Figure 2. The TOE's main components are the card operating system (either a native OS, or in the case of JavaCard a combination of OS and applet), and the file-system. Note that *file-system* denotes here an abstract structure conformant to [ISO7816-4] to store datagroups, and the internal implementation of the file-system on the TOE can be completely different depending on the specific product.

The TOE provides certain security functionality (TSF). This security functionality consists here mainly of algorithms and protocols that control access to, generation of, and modification of data stored in the file-system. Common Criteria [CC1] defines TSF as

> *combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.*

From this definition it is clear, that only those combined functionality of the TOE that is related to the enforcement of the SFRs is the TSF, but that the TSF does not correspond to the TOE's functionality *in general*. The TOE as a whole usually also provides functionality to (end-)users. To provide this functionality, the TOE often makes use of it's security functionality. As an example, the TSF might functionally provide an algorithm that employs random numbers to the user. To ensure correctness and security of this algorithm, the TSF might have methods for self-protection, or internal tests to ensure that random numbers are generated w.r.t. a certain metric. Such TSF is usually not directly accessible and does not belong to the TOE's general functionality provided to users. Therefore, the TOE's security functionality and the TOE's functionality in general need not to always coincide and must be viewed as *separate*. SFRs within this PP define requirements on the TSF, but usually not on the TOE's functionality in general. This fact is important to note for using this PP and for evaluation.

1.3.4 Security Targets, Strict Conformance, and Evaluation

The intended use of this PP is as follows:

Step 1:
In a first step, one security target should be written that claims strict conformance to this protection profile. Since all SFRs within this protection profile are then included in that security target and thus are subject to evaluation, and since the filesystem is part of the TOE, a filesystem with applications, i.e. (test) datagroups, has to be created. This allows thorough evaluation w.r.t. this protection profile including *all* SFRs; this in particular includes *all* access control mechanisms and cryptographic functions.

Step 2:
Such a TOE however will likely not coincide with a finished product as intended for end-users. Each such product will have a different filesystem. In a second step, for each such product a separate security target should be created. Such a security target should claim strict conformance to this protection profile, and, in addition precisely define the respective filesystem and data related to that.

Each of these security targets is subject to evaluation. Note that these security targets' only difference to the one of Step 1 is the filesystem: Depending on the product, the filesystem may not contain all applications, i.e. not all files compared to the TOE of *Step 1*. However whereas not all datagroups will be present, in order to achieve strict conformity with this protection profile, *all mechanisms*, i.e. TSF such as access controls, and cryptographic operations described in the SFRs of this PP *must* be implemented and available in the card operating system in principal, even though the functionality may not be usable (and hence also not accessible for end-users) without the appropriate filesystem in the respective product configuration.

Concerning the evaluation, on a superficial level this looks like a duplication of work, as for each product yet another evaluation w.r.t. each of these security targets has to be conducted. In order to assess the fulfillment of all SFRs however, evaluation results of *Step 1* should be reused to the *highest extend possible* to assess conformity. This in particular includes assessing conformity to those SFRs that require for evaluation the

presence of certain datagroups that might not be present in the respective filesystem for the given product. Conformity w.r.t. those SFRs is still given, since the *mechanisms* are still available in principal and
310 implemented; it is only the lack of corresponding files and related data that potentially creates a hurdle during evaluation, and this is addressed by applying the evaluation results of *Step 1*.

Some SFRs explicitly require the TSF to provide certain functionality. Formulations usually include “The TSF shall allow...”, “The TSF shall be capable...”., or “The TSF shall provide...”. This is to be understood in the sense that, as mentioned above, the TOE provides these TSF, and these TSF are subject to evaluation, but whether
315 they are accessible as general functionality in the life cycle after personalization, i.e. to (end) users, depends on the filesystem. For example for a TOE where no EAC1-protected data are stored and thus no application is present, the EAC1 protocol might not be accessible to end-users, since the file-system does not include any CA1 keys. This is even though the TOE is technically capable of performing EAC1, i.e. the functionality is in principal present in the card operating system.

320 Affected SFRs in particular include those from the families FIA and FMT.

Note that this is in no contradiction to strict conformance to this protection profile, since not only is all the evaluated TSF still available in principal, but also limiting outside access to functionality that allows to gather user data does never *decrease* security.

2 Conformance Claims

2.1 CC Conformance Claim

This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, [CC1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012, [CC2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012, [CC3]

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 4, September 2012, [CC4]

has to be taken into account.

2.2 PP Claim

This PP claims strict conformance to

- Common Criteria Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.01, 2012-01, BSI-CC-PP-0059-2009-MA-01, [SSCDPP]
  Application note 7: This conformance claim covers the part of the security policy for the *eSign* application of the TOE corresponding to the security policy defined in [SSCDPP], and hence is applicable, if the *eSign* application is operational. In addition to [SSCDPP], the current PP specifies authentication and communication protocols (at least PACE) that have to be used for the *eSign* application of the TOE. These protocols contribute to secure Signature Verification Data (SVD) export, Data To Be Signed (DTBS) import, and Verification Authentication Data (VAD) import functionality.
- 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, [EAC2PP]

Since the last two above claim strict conformance to [PACEPP], this PP 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].

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

2.3 Package Claim

The current PP is conformant to the following packages:

1. Assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in [CC3].

2.4 Conformance Rationale

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

- The TOE type of this PP is the same[4] 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 [TR03110-1] and [TR03110-2], and for the eSign application additionally representing a combination of hardware and software configured to securely create, use and manage signature-creation data.
- The security problem definition (SPD) of this PP contains the SPD of the claimed PPs. The SPD contains all threats, organizational security policies and assumptions of the claimed PPs and identifies additional threats T.InconsistentSec and T.Interfere.
- The security objectives for the TOE in this PP include all the security objectives for the TOE of the claimed PPs, and add the security objective OT.Non_Interfere. This objective does not weaken the security objectives of the claimed PPs.
- The security objectives for the operational environment in this PP include all security objectives for the operational environment of the claimed PPs.
- The SFRs specified in this PP include all security functional requirements (SFRs) specified in the claimed PPs. We especially point to the following three refined SFRs within this PP:
  The SFR **FIA_UAU.1/SSCDPP** is redefined from [SSCDPP] by additional assignments. Note that 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-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**.
- The SARs specified in this PP are the same as specified in the claimed PPs or extend them.

2.5 Conformance Statement

This PP requires strict conformance of any ST or PP claiming conformance to it.

4 see also the justification in Chapter 1.2.3.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

3.1.1.1 Primary Assets

As long as they are in the scope of the TOE, the primary assets to be protected by the TOE are listed below. For a definition of terms used, but not defined here, see the Glossary.

Authenticity of the Electronic Document's Chip

385 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

390 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
395 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
400 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
405 [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
410 the asset defined in [PACEPP]. As for confidentiality, note that even though not each data element being

transferred represents a secret, [TR03110-1], [TR03110-2] resp. require confidentiality of all transferred data by secure messaging in encrypt-then-authenticate mode. This asset also includes “DTBS” of [SSCDPP].

3.1.1.2 Secondary Assets

In order to achieve a sufficient protection of the primary assets listed above, the following secondary assets also have to be protected by the TOE.

Accessibility to the TOE Functions and Data only for Authorized Subjects

415 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

Electronic Document Communication Establishment Authorization Data

Restricted-revealable authorization information for a human user being used for verification of the
420 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.

425 *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
430 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

435 *Application Note 8*: The above secondary assets represent TSF and TSF-Data in the sense of CC.

3.1.2 Subjects

This protection profile considers the following external entities and subjects:

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
440 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 a self-signed CSCA certificate that has to be distributed to other
445 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
450 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)
455 An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see [TR03110-3].

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
460 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
465 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.

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
470 implements the terminal part of the PACE protocol and authenticates itself to the electronic document using a shared password (CAN, eID-PIN, eID-PUK or MRZ). A PACE terminal is not allowed reading sensitive user data.

Personalization Agent
An 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
475 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], [TR03110-3]) 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 or contact-based 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.

3.2 Threats

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

T.InconsistentSec Inconsistency of security measures

Adverse action: 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.

Threat agent: having high attack potential, being 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

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

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

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

T.AdvancedTracing Advanced Tracing and Group Key Compromise

Adverse action: 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.

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

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

3.2.1 Threats from [EAC1PP]

This PP includes the following threats from [EAC1PP]. They concern EAC1-protected data.

- **T.Counterfeit**
- 520 **T.Read_Sensitive_Data**

Due to identical definitions and names they are not repeated here. For the remaining threats from [EAC1PP], cf. Chapter 3.2.3.

3.2.2 Threats from [EAC2PP]

This PP includes the following threats from the [EAC2PP]. They concern EAC2-protected data.

- **T.Counterfeit/EAC2**
- 525 **T.Sensitive_Data**

Due to identical definitions and names, they are not repeated here.

3.2.3 Threats from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP], and thus include the threats formulated in [PACEPP]. We list each threat only once here. Due to identical definitions and names, their definitions are not repeated here.

- **T.Abuse-Func**
- 530 **T.Eavesdropping**
- **T.Forgery**
- **T.Information_Leakage**
- **T.Malfunction**
- **T.Phys-Tamper**
- 535 **T.Skimming**
- **T.Tracing**

3.2.4 Threats from [SSCDPP]

The current PP also includes all threats of [SSCDPP]. These items are applicable if the eSign application is operational.

- **T.DTBS_Forgery**
- 540 **T.Hack_Phys**
- **T.SCD_Derive**
- **T.SCD_Divulge**
- **T.Sig_Forgery**

- **T.SigF_Misuse**
- **T.SVD_Forgery**

Due to identical definitions and names, their definitions are not repeated here.

3.3 Organizational Security Policies

The TOE 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 PP includes the OSPs from the claimed protection profiles as listed below and provides no further OSPs.

3.3.1 OSPs from [EAC1PP]

This PP includes the following OSPs from [EAC1PP], if the TOE contains EAC1-protected data.

- **P.Personalisation**
- **P.Sensitive_Data**

Due to identical definitions and names, they are not repeated here. For the remaining OSPs from [EAC1PP], see the next sections.

3.3.2 OSPs from [EAC2PP]

This PP includes the following OSPs from [EAC2PP]. They mainly concern EAC2-protected data.

- **P.EAC2_Terminal**
- **P.RestrictedIdentity**
- **P.Terminal_PKI**

Due to identical definitions and names, their definitions are not repeated here. For the remaining OSPs from [EAC2PP], cf. the next section.

3.3.3 OSPs from [PACEPP]

This PP includes the following OSPs from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP]. We list each OSP only once here. Due to identical definitions and names, their definitions are not repeated here as well.

- **P.Card_PKI**
- **P.Manufact**
- **P.Pre-Operational**
- **P.Terminal**
- **P.Trustworthy_PKI**

3.3.4 OSPs from [SSCDPP]

The current PP also includes all OSPs of [SSCDPP]. They are applicable, if the eSign application is included.

- **P.CSP_QCert**
- **P.QSign**

- **P.Sig_Non-Repud**
- **P.Sigy_SSCD**

Due to identical definitions and names, their definitions are not repeated here.

3.3.5 Additional OSPs

The next OSP addresses the need of a policy for the document manufacturer. It is formulated akin to [ICPP].

P.Lim_Block_Loader
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.

3.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. This PP includes the assumptions from the claimed protection profiles as listed below and defines no further assumptions.

3.4.1 Assumptions from [EAC1PP]

This PP includes the following assumptions from the [EAC1PP]. They concern EAC1-protected data.

- **A.Auth_PKI**
- **A.Insp_Sys**

Due to identical definitions and names, their definitions are not repeated here. For the remaining assumptions from [EAC1PP], see the next sections.

3.4.2 Assumptions from [EAC2PP]

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

3.4.3 Assumptions from [PACEPP]

This PP includes the following assumptions from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

- **A.Passive_Auth**

Due to an identical definition and name, its definition is not repeated here as well.

3.4.4 Assumptions from [SSCDPP]

The current PP also includes all assumptions of [SSCDPP]. These items are applicable, if the eSign application is included.

- **A.CGA**
- **A.SCA**

Due to identical definitions and names their definitions are not repeated here.

4 Security Objectives

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
600 production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE, addressing the aspects of identified threats to be countered by the TOE, and organizational security policies to be met by the TOE.

OT.Non_Interfere No interference of Access Control Mechanisms
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
605 interference of one access control mechanism with another one.

4.1.1 Security Objectives for the TOE from [EAC1PP]

This PP includes the following additional security objectives for the TOE from [EAC1PP] that are not included in [PACEPP]. They concern EAC1-protected data.

- **OT.Chip_Auth_Proof**
- **OT.Sens_Data_Conf**

610 Due to identical definitions and names, their definitions are not repeated here. For the remaining security objectives from [EAC1PP], see the next sections.

In addition, the following security objective is defined here:

OT.Chip_Auth_Proof_PACE_CAM Proof of the electronic document's chip authenticity
The TOE must support the terminals to verify the identity and authenticity of the electronic document's chip as issued by the identified issuing State or Organization by means of the-PACE-Chip Authentication
615 Mapping (PACE-CAM) as defined in [ICAO9303]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

Application note 9: PACE-CAM enables much faster authentication of the of the chip than running PACE with General Mapping (according to [TR03110-1]) followed by CA1. OT.Chip_Auth_Proof_PACE_CAM is intended to require the Chip to merely provide an additional means – with the same level of security –
620 of authentication.

4.1.2 Security Objectives for the TOE from [EAC2PP]

This PP includes the following additional security objectives for the TOE from [EAC2PP] that are not included in [PACEPP]. They concern EAC2-protected data.

- **OT.AC_Pers_EAC2**
- **OT.CA2**
- 625 **OT.RI_EAC2**
- **OT.Sens_Data_EAC2**

Due to identical definitions and names, their definitions are not repeated here. In addition, the next security objective is added:

OT.CA3 Protection against advanced tracing techniques using Chip Authentication 3
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. [TR03110-2-v2.20]).

4.1.3 Security Objectives for the TOE from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives are included as well. We list them only once here.

- **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**

Due to identical definitions and names, their definitions are not repeated here.

4.1.4 Security objectives for the TOE from [SSCDPP]

The current PP also includes all security objectives for the TOE of [SSCDPP]. These items are applicable, if an eSign application is included.

- **OT.DTBS_Integrity_TOE**
- **OT.EMSEC_Design**
- **OT.Lifecycle_Security**
- **OT.SCD_Secrecy**
- **OT.SCD_SVD_Corresp**
- **OT.SCD_Unique**
- **OT.SCD/SVD_Gen**
- **OT.Sig_Secure**
- **OT.Sigy_SigF**
- **OT.Tamper_ID**
- **OT.Tamper_Resistance**

Due to identical definitions and names, their definitions are not repeated here as well. Note that all are formally included here, but careful analysis reveals that 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 [PACEPP].

4.1.5 Additional Security Objectives for the TOE

A loader is a part of the chip operating system that allows to load data, i.e. the file-system/applet containing (sensitive) user data, TSF data etc. into the Flash or EEPROM memory after delivery of the smartcard to the
665 document manufacturer.

The following objective for the TOE addresses limiting the availability of the loader, and is formulated akin to [ICPP].

OT.Cap_Avail_Loader
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.

4.2 Security Objectives for the Operational Environment

4.2.1 Security objectives from [EAC1PP]

670 This PP includes the following security objectives for the TOE from the [EAC1PP]. They mainly concern EAC1-protected data.

- **OE.Auth_Key_Travel_Document**
- **OE.Authoriz_Sens_Data**
- **OE.Exam_Travel_Document**
675 - **OE.Ext_Insp_Systems**
- **OE.Prot_Logical_Travel_Document**

Due to identical definitions and names, their definitions are not repeated here. For the remaining ones, see the next sections.

4.2.2 Security Objectives from [EAC2PP]

This PP includes the following security objectives for the TOE from the [EAC2PP]. They mainly concern
680 EAC2-protected data.

- **OE.Chip_Auth_Key**
- **OE.RestrictedIdentity**
- **OE.Terminal_Authentication**

Due to identical definitions and names, their definitions are not repeated here. For the remaining ones, see
685 the next section.

4.2.3 Security Objectives from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives on the operational environment are included as well. We repeat them only once here.

- **OE.Legislative_Compliance**
- **OE.Passive_Auth_Sign**

- **OE.Personalisation**
- **OE.Terminal**
- **OE.Travel_Document_Holder**

Due to identical definitions and names, they are not repeated here as well.

4.2.4 Security Objectives from [SSCDPP]

The current PP also includes all security objectives for the TOE of [SSCDPP]. These items are applicable, if an eSign application is included.

- **OE.CGA_QCert**
- **OE.DTBS_Intend**
- **OE.DTBS_Protect**
- **OE.HID_VAD**
- **OE.Signatory**
- **OE.SSCD_Prov_Service**
- **OE.SVD_Auth**

Due to identical definitions and names, their definitions are not repeated here.

4.2.5 Additional Security Objectives for the Environment

The following objective on the environment is defined akin to the objective from [ICPP].

OE.Lim_Block_Loader
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.

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.

4.3 Security Objective Rationale

Table 2 provides an overview of the security objectives' coverage. According to [CC1], the tracing between security objectives and the security problem definition must ensure that 1) *each security objective traces to at least one threat, OSP and assumption*, 2) *each threat, OSP and assumption has at least one security objective tracing to it*, and 3) *the tracing is correct* (i.e. the main point being that security objectives for the TOE do not trace back to assumptions).

This is illustrated in the following way:

1) can be inferred for security objectives from claimed PPs by looking up the security objective rationale of the claimed PPs and for newly introduced security objectives (i.e. **OE.Lim_Block_Loader** and

OT.Cap_Avail_Loader, OT.CA3 and OT.Chip_Auth_Proof_PACE_CAM) by checking the *columns* of Table 2,

2) can be inferred for threats, OSPs and assumptions from the claimed PPs by looking up the security objective rationale of the claimed PPs and for newly introduced threats, OSPs and assumptions by checking the rows of Table 2, and

3) simply by checking the *columns* of Table 2 and the security objective rationales from the claimed PPs.

	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Cap_Avail_Loader	OT.Chip_Auth_Proof_PACE_CAM	OT.CA3	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Non_Interfere	OT.Sens_Data_Conf (EAC1PP)	OT.Sens_Data_EAC2	OE.Lim_Block_Loader
T.InconsistentSec	x	x	x			x	x	x	x	x	x	x
T.Interfere									x			
T.Counterfeit				x								
T.Counterfeit/EAC2					x							
T.AdvancedTracing					x							
P.Lim_Block_Loader			x						x			x

Table 2: Security Objective Rationale

The threat **T.InconsistentSec** addresses attacks on the confidentiality and the integrity of user data stored on the TOE, facilitated by the data not being protected as intended.
OT.AC_Pers and OT.AC_Pers_EAC2 define the restriction on writing or modifying data;
OT.Data_Authenticity, OT.Data_Confidentiality, OT.Data_Integrity, OT.Sens_Data_Conf (from [EAC1PP]), and OT.Sens_Data_EAC2 require the security of stored user data as well as user data that are transferred between the TOE and a terminal to be secure w.r.t. authenticity, integrity and confidentiality.
OT.Non_Interfere requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.
OT.Cap_Avail_Loader requires the TOE to provide limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data.
OE.Lim_Block_Loader requires the manufacturer to protect the loader functionality against misuse, limit the capability of the loader, and terminate irreversibly the loader after intended usage of the loader.

The combination of these security objectives cover the threat posed by **T.InconsistentSec**.

The threat **T.Interfere** addresses the attack on user data by exploiting the unintended interference of security protocols. This is directly countered by OT.Non_Interfere, requiring the TOE's access control mechanisms to be implemented consistently, and their implementations to not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

The threat **T.Counterfeit** (from [EAC1PP]) is countered in [EAC1PP] by OT.Chip_Auth_Proof. That security objectives addresses the implementation of the Chip Authentication Protocol Version 1 (CA1) and thus counters the thread of counterfeiting an electronic document containing an ePassport application. Here, the additional security objective for the TOE OT.Chip_Auth_Proof_PACE_CAM is introduced. It ensures that the chip in addition to CA1 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which

supports the same security functionality as CA1 does. PACE-CAM enables much faster authentication of the of the chip than running PACE with general mapping followed by CA1.

The threat **T.Counterfeit/EAC2** (from [EAC2PP]) is here countered with OT.CA3 in addiction to OT.CA2
755 ([EAC2PP]),, since Chip Authentication 3 provides a superset of functions of Chip Authentication 2.

The threat **T.AdvancedTracing** is countered with OT.CA3. The main feature of Chip Authentication 3 is that cryptographic mechanisms are employed to provides pseudonymity of the electronic document without the need to use the same keys on several chips. This directly counters the described threat.

The OSP **P.Lim_Block_Loader** addresses limiting the capability and blocking the availability of the Loader in
760 order to protect stored data from disclosure and manipulation. This is addressed by OT.Cap_Avail_Loader, which requires the TOE to provide a limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data; by OT.Non_Interfere, which requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of
765 one access control mechanism with another one; and by OE.Lim_Block_Loader, which requires the manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

5 Extended Components Definition

This PP includes all extended components from the claimed PPs. This includes

- FAU_SAS.1 from the family FAU_SAS from [PACEPP]
- FCS_RND.1 from the family FCS_RND from [PACEPP]
- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM from [PACEPP]
- FPT_EMS.1 from the family FPT_EMS from [PACEPP]
- FIA_API.1 from the family FIA_API from [EAC2PP]

For precise definitions we refer to [PACEPP] and [EAC2PP].

6 Security Requirements

775 This part defines 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 must satisfy in order to meet the security objectives for the TOE.

Common Criteria allows several operations to be performed on security requirements on the component level: *refinement*, *selection*, *assignment* and *iteration,* cf. sec. 8.1 of [CC1]. Each of these operations is used in
780 this PP.

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 words are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by CC in stating a requirement.
785 Selections that have been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection has to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted as underlined text.
790 Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized *like this*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. For the sake of better
795 readability, the iteration operation may also be applied to a non-repeated single component in order to indicate that such component belongs to a certain functional cluster. In such a case, the iteration operation is applied to only one single component.

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 resp. renamed in the following way:

800 /EAC1PP or /XXX_EAC1PP [EAC1PP],

/EAC2PP or /XXX_EAC2PP for [EAC2PP],

and /SSCDPP or /XXX_SSCDPP for [SSCDPP].

6.1 Security Functional Requirements

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
805 inconsistency.

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

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.

Thus internal consistency is not violated.

Last, we remark that compared to [EAC2PP] the following references in SFRs have been updated:

- The reference [ICAO9303] was updated from the sixth to the seventh edition.
- The document *Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.1, 15. April 2014.* was replaced with [ICAO9303], since that technical report has been included in the seventh edition of [ICAO9303].

Since the content of the specifications has not changed, we do not explicitly mark these (editorial) refinements in the SFRs.

6.1.1 Class FCS

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**

The following SFR is new and concerns cryptographic support for enhancements of [EAC2PP] (Chip Authentication 3).

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 by FCS_COP.1/PACE_ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC2PP

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[5] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR03110-2-v2.20][6].

Application note 10: 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}.

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 by FCS_CKM.1/C

FCS_CKM.4 Cryptographic key destruction
fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/CA3

The TSF shall perform the Chip Authentication 3 (CA3) protocol[7] in accordance with a specified cryptographic algorithm CA3[8] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following:[TR03110-2-v2.20][9].

Application Note 11: 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** [TR03110-2-v2.20].

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, but listed here for the sake of completeness)
- **FCS_COP.1/PACE_ENC_EAC1PP**
- **FCS_COP.1/PACE_MAC_EAC1PP**
  Application note 12: Note that national regulations w.r.t. key sizes and algorithms may further restrict the choice of algorithms and key sizes defined in the above two SFRs.
- **FCS_RND.1/EAC1PP**
  (equivalent to FCS_RND.1/EAC2PP, but listed here 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**

5 [assignment: *cryptographic key generation algorithm*]
6 [assignment: *list of standards*]
7 [assignment: *list of cryptographic operations*]
8 [assignment: cryptographic algorithm]
9 [assignment: *list of standards*]

The following SFR is new and concerns cryptographic support for ePassport applications in combination with [EAC1PP].

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:

885 [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

fulfilled by FCS_COP.1/PACE_ENC_EAC1PP and FCS_COP.1/PACE_MAC_EAC1PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC1PP

FCS_CKM.1.1/CAM
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation
890 algorithm PACE-CAM in combination with PACE-GM[10] and specified cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [ICAO9303][11].

Application note 13: 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
895 this value together with chip authentication public key to the card; cf. [ICAO9303].

FCS_COP.1/CAM Cryptographic Operation – PACE-CAM

Hierarchical to:
No other components.

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

900 FCS_CKM.4 Cryptographic key destruction
fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/CAM
The TSF shall perform the PACE-CAM protocol[12] in accordance with a specified cryptographic algorithm PACE-CAM[13] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR03110-2-v2.20][14].

905 *Application Note* 14: Whereas FCS_CKM.1/CAM addresses the Diffie-Hellman based key-derivation, this SFR is concerned with the correct implementation and execution of the whole PACE-CAM protocol. Note that in particular the last protocol step to authenticate the chip towards the terminal is an essential part of the protocol, and not addressed in FCS_CKM.1/CAM.

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

- **FCS_CKM.1/SSCDPP**

10 [assignment: *cryptographic key generation algorithm*]
11 [assignment*: list of standards*]
12 [assignment: *list of cryptographic operations*]
13 [assignment: *cryptographic algorithm*]
14 [assignment: *list of standards*]

- **FCS_CKM.4/SSCDPP**
- **FCS_COP.1/SSCDPP**

6.1.2 Class FIA

Table 3 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE
PACE protocol	FIA_UAU.1/PACE_EAC2PP FIA_UAU.5/PACE_EAC2PP FIA_AFL.1/Suspend_PIN_EAC2PP FIA_AFL.1/Block_PIN_EAC2PP FIA_AFL.1/PACE_EAC2PP FIA_AFL.1/PACE_EAC1PP
PACE-CAM protocol	SFRs above for the PACE part; in addition for the Chip Authentication Mapping (CAM): FIA_API.1/PACE_CAM FIA_UAU.5/PACE_EAC1PP
Terminal Authentication Protocol version 2	FIA_UAU.1/EAC2_Terminal_EAC2PP FIA_UAU.5/PACE_EAC2PP
Chip Authentication Protocol version 2	FIA_API.1/CA_EAC2PP FIA_UAU.5/PACE_EAC2PP FIA_UAU.6/PACE_EAC2PP
Terminal Authentication Protocol version 1	FIA_UAU.1/PACE_EAC1PP FIA_UAU.5/PACE_EAC1PP
Chip Authentication Protocol version 1	FIA_API.1/EAC1PP FIA_UAU.5/PACE_EAC1PP FIA_UAU.6/EAC_EAC1PP
Chip Authentication Protocol version 3	FIA_API.1/CA3 FIA_UAU.5/PACE_EAC2PP (refined) FIA_UAU.6/CA3
Restricted Identification	FIA_API.1/RI_EAC2PP
eSign-PIN	FIA_UAU.1/SSCDPP

Table 3: Overview of authentication SFRs

6.1.2.1 SFRs for EAC2-protected Data

915 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**
- 920 • **FIA_API.1/RI_EAC2PP**
- **FIA_UID.1/PACE_EAC2PP**

- **FIA_UID.1/EAC2_Terminal_EAC2PP**
  Application note 15: 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.6/CA_EAC2PP**
- **FIA_AFL.1/PACE_EAC2PP**
- **FIA_UAU.6/PACE_EAC2PP**

The following SFRs are new or refined from [EAC2PP] and concern cryptographic support for enhancements of [EAC2PP] (Chip Authentication 3).

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 [TR03110-2-v2.20][15], to prove the identity of the TOE[16].

FIA_UAU.5/PACE_EAC2PP Multiple Authentication Mechanisms

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_UAU.5.1/PACE_EAC2PP
The TSF shall provide

1. PACE protocol according to [**TR03110-2**],
2. Passive Authentication according to [ICAO9303]
3. Secure messaging ~~**in MAC-ENC mode**~~ according to [**TR03110-3**]
4. Symmetric Authentication Mechanism based on [selection: *AES or other approved algorithms*][17]
5. Terminal Authentication 2 protocol according to [TR03110-2],
6. Chip Authentication 2 according to [TR03110-2][18]
7. Chip Authentication 3 according to [TR03110-2-v2.20][19]
8. [assignment: *list of multiple authentication mechanisms*]

15 [assignment: *authentication mechanism*]
16 [assignment: *authorized user or role, or of the TOE itself*]
17 restricting the [selection: *Triple-DES, AES or other approved algorithms*]
18 Passive Authentication using SO_C is considered to be part of CA2 within this PP.
19 [assignment: *list of multiple authentication mechanisms*]

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 [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]
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[20].
6. [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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 each command sent to the TOE after a successful run of Chip Authentication 3 shall be verified as being sent by the EAC2 terminal[21].

6.1.2.2 SFRs for EAC1-protected data

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

- **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, but listed here 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, but listed here for the sake of completeness)

20 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
21 [assignment: *list of conditions under which re-authentication is required*]

The following SFRs are refined from [EAC1PP]. Refinements address mainly the PACE-CAM protocol.

FIA_UID.1/PACE_EAC1PP Timing of identification

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_UID.1.1/PACE_EAC1PP
The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to **[TR03110-1]**,
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 [TR03110-1] **or the Chip Authentication Mapping (PACE-CAM) according to [ICAO9303]**,
5. to carry out the Terminal Authentication Protocol v.1 according to [TR03110-1] **resp. according to [ICAO9303] if PACE-CAM is used.**[22]
6. [assignment: *list of TSF-mediated actions*].

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.

Application note 16: The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol by referencing [ICAO9303]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

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 [selection: *Triple-DES, AES or other approved algorithms*]
5. Terminal Authentication Protocol v.1 according to [TR03110-1][23]

to support user authentication.

22 [assignment: *list of TSF-mediated actions*]
23 [assignment: *list of multiple authentication mechanisms*]

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 Personalisation Agent by [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*].
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**[24].
5. [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Application note 17: The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol by referencing [ICAO9303]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

The following SFR is newly defined in this PP and addresses the PACE-CAM protocol.

FIA_API.1/PACE_CAM Authentication Proof of Identity

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_API.1.1/PACE_CAM
The TSF shall provide the protocol PACE-CAM [ICAO9303][25], to prove the identity of the TOE[26].

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**

6.1.2.3 SFRs concerning eSign-applications

The next claimed SFR is refined from [SSCDPP] by additional assignments. Note that this does not violate strict conformance to [SSCDPP].

FIA_UAU.1/SSCDPP

Hierarchical to:
No other components.

24 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
25 [assignment: *authentication mechanism*]
26 [assignment: *authorised user or role, or of the TOE itself*]

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

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/SSCD,
3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2PP and FTP_ITC.1/CA3 respectively,
4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2PP and FTP_ITC.1/CA3 respectively,
5. [assignment: *list of additional TSF-mediated actions*]

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.

6.1.3 Class FDP

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.

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 exist.

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

Hierarchical to:
No other components.

Dependencies:
FDP_ACC.1 Subset access control
fulfilled by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP
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[27] to objects based on the following:

27 [assignment: *access control SFP*]

1) Subjects:

a) Terminal,

b) PACE terminal,

c) EAC2 terminal [assignment: *list of EAC2 terminal types*],

d) EAC1 terminal[28];

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)[29][30].

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 [TR03110-2] **and/or** [**ICAO9303**], as required by FIA_UAU.1/PACE.[31]

FDP_ACF.1.3/TRM

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[32]

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, or to use any user data stored on the electronic document.[33]
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:
   [assignment: *list of rules for PIN management chosen from[TR03110-2]*].
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.

28 [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes*] (added using open assignment of [EAC2PP])

29 [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes*] (added using open assignment of [EAC2PP])

30 [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes*] (all bullets in FDP_ACF.1.1/TRM w.r.t. [CC2])

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

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

33 note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.

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 [TR03110-2]. 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 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. [TR03110-1] 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).[34]

Application note 18: The above definition is based on FDP_ACF.1/TRM_EAC2PP. We argue that it covers FDP_ACF.1/TRM_EAC1PP as well. Subject 1b and 1d 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 3a) *Terminal Authorization Level* here subsumes the explicitly enumerated attributes 3a) and 3b) 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 [TR03110-2]. However the references are compatible as justified in [EAC2PP], yet both are mentioned here since [TR03110-2] is the primary norm for an eID application, whereas [ICAO9303] 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.
References are changed in FDP_ACF.1.2/TRM_EAC1PP. It is already justified in [EAC2PP] that definitions in [TR03110-2] and [ICAO9303] are compatible.
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_EAC1PP 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 conflicts 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 w.r.t. 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]. None of this conflicts with strict conformance.
The dependency of this SFR is met by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP. Note

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

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 2b) of FDP_ACF.1.1/TRM must be restricted as well according to the SFP, otherwise access to user data is impossible to enforce.

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 19: 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**

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, but listed here for the sake of completeness)
- **FDP_UIT.1/TRM_EAC1PP**
  (equivalent to FDP_UIT.1/TRM_EAC2PP, but listed here for the sake of completeness)

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**

6.1.4 Class FTP

The following SFRs are imported from [EAC2PP].

- **FTP_ITC.1/PACE_EAC2PP**
- **FTP_ITC.1/CA_EAC2PP**

FTP_ITC.1/CA3 Inter-TSF trusted channel after CA3

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 [TR03110-2-v2.20].**

FTP_ITC.1.2/CA3
The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal** [35] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA3
The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 3. [36]

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

- **FTP_ITC.1/PACE_EAC1PP**

6.1.5 Class FAU

The following SFR is imported due to claiming [EAC2PP]. It concerns applications with EAC2-protected data.

- **FAU_SAS.1/EAC2PP**

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

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

6.1.6 Class FMT

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.

35 [selection: *the TSF, another trusted IT product*]
36 [assignment: *list of functions for which a trusted channel is required*]

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 ePassport application is active
9. Electronic document holder.[37]

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

The next 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 MT_SMR.1/PACE_EAC1PP into to by FMT_SMR.1.
- **FMT_MTD.1/DATE_EAC2PP**
- **FMT_MTD.1/PA_EAC2PP**
- **FMT_MTD.1/SK_PICC_EAC2PP**
  Application note 20: The formulation *Chip Authentication Private Key(s)* MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{ICC,1}$, $SK_{ICC,2}$) as well.
- **FMT_MTD.1/KEY_READ_EAC2PP**
  Application note 21: The formulation *Chip Authentication Private Key(s)* MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{ICC,1}$, $SK_{ICC,2}$) as well.
- **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**
  Application note 22: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

37 [assignment: *the authorized identified roles*]

- **FMT_LIM.2/EAC2PP**
  Application note 23: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.
- **FMT_MTD.1/INI_ENA_EAC2PP**
- **FMT_MTD.1/INI_DIS_EAC2PP**

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, but listed here for the sake of completeness.
- **FMT_LIM.2/EAC1PP**
  This SFR is equivalent to FMT_LIM.2/EAC2PP, but listed here for the sake of completeness.
- **FMT_MTD.1/INI_ENA_EAC1PP**
  (equivalent to FDP_MTD.1/INI_ENA_EAC2PP, but listed here for the sake of completeness)
- **FMT_MTD.1/INI_DIS_EAC1PP**
  (equivalent to FDP_MTD.1/INI_DIS_EAC2PP, but listed here for the sake of completeness)
- **FMT_MTD.1/CVCA_INI_EAC1PP**
- **FMT_MTD.1/CVCA_UPD_EAC1PP**
- **FMT_MTD.1/DATE_EAC1PP**
  This SFR is equivalent to FMT_MTD.1/DATE_EAC2PP . 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**
- **FMT_MTD.1/KEY_READ_EAC1PP**
- **FMT_MTD.3/EAC1PP**

The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the security management of an *eSign* application.

- **FMT_SMR.1/SSCDPP**
- **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**

The following SFRs are defined here. The concern loading applications onto the IC during manufacturing and relate directly to OT.Cap_Avail_Loader.

FMT_LIM.1/Loader Limited Capabilities

Hierarchical to:
No other components

Dependencies:
FMT_LIM.2/Loader Limited availability

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 [assignment: *action*] does not allow stored user data to be disclosed or manipulated by unauthorized users.[38]

Application note 24: 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.

FMT_LIM.2/Loader Limited Availability

Hierarchical to:
No other components

Dependencies:
FMT_LIM.1/Loader Limited capabilities

FMT_LIM.2.1/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 [assignment: *action*].[39]

Application note 25: 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.

6.1.7 Class FPT

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 TOE Emanation

Hierarchical to:
No other components.

Dependencies:
No dependencies.

38 [assignment: *Limited capability and availability policy*]
39 [assignment: *Limited capability and availability policy*]

FPT_EMS.1.1/EAC2PP

The TOE shall not emit [*assignment: types of emissions*] in excess of [assignment: *specified limits*] enabling access to

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 keys (SK_{PICC}), **both CA2 and CA3,**
4. the PIN, PUK,
5. the additional Chip Authentication 3 private sector keys ($SK_{ICC,1}$ and $SK_{ICC,2}$)[40]
6. [assignment: *list of types of TSF data*]

and

7. the Restricted Identification private key(s) SK_{ID},
8. [assignment: *list of types of user data*].

FPT_EMS.1.2/EAC2PP

The TSF shall ensure any users are unable to use the following interface electronic document's contactless/**contact-based interface** and circuit contacts to gain access to

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(s) (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 $SK_{ICC,2}$)[41]
7. [assignment: *list of types of TSF data*]

and

8. the Restricted Identification private key(s) SK_{ID},
9. [assignment: *list of types of user data*].

Application note 26: Note that related to *Application Note 6*, 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 be protected is a superset of the ones of the SFR from [EAC2PP]. Hence, the requirement is more 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.

- **FPT_FLS.1/EAC2PP**
- **FPT_TST.1/EAC2PP**
- **FPT_PHP.3/EAC2PP**

40 [assignment: *list of types of TSF data*]
41 [assignment: *list of types of TSF data*]

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, but listed here for the sake of completeness)
- **FPT_FLS.1/EAC1PP**
  (equivalent to FPT_FLS.1/EAC2PP, but listed here for the sake of completeness)
- **FPT_PHP.3/EAC1PP**
  (equivalent to FPT_PHP.3/EAC2PP, but listed here for the sake of completeness)

FPT_EMS.1/EAC1PP Emanation

Hierarchical to:
No other components

Dependencies:
No dependencies.

FPT_EMS.1.1/EAC1PP
The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to

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[42]
5. [assignment: *list of types of TSF data*],
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key[43] and
8. [assignment: *list of types of user data*]

FPT_EMS.1.2/EAC1PP
The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to

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[44]
5. [assignment: *list of types of TSF data*],
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key[45]
8. [assignment: *list of types of user data*]

Application note 27: 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

42 [assignment: *list of types of TSF data*]
43 [assignment: *list of types of TSF data*]
44 [assignment: *list of types of TSF data*]
45 [assignment: *list of types of TSF data*]

in order not to confuse Chip Authentication 1 with 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.
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 SK_{PICC} by computing $SK_{PICC} = i(CA_{PICC})$ ° $SK_{Map,PICC}$-PACE-CAM.

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_FPT_TST.1/EAC2PP)

6.2 Security Assurance Requirements for the TOE

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

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

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.

	OT.Chip_Auth_Proof (EAC1PP)	OT.Chip_Auth_Proof_PACE_CAM	OT.Sens_Data_Conf (EAC1PP)	OT.AC_Pers_EAC2	OT.CA3	OT.Sens_Data_EAC2	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.AC_Pers*	*OT.Prot_Inf_Leak*	OT.Non_Interfere	OT.SCD/SVD_Gen (SSCDPP)	OT.Sigy_SigF (SSCDPP)	OT.Cap_Avail_Loader	*OT.RI_EAC2*
Class FCS																	
FCS_CKM.1/CA3					x	x	x	x	x								
FCS_COP.1/CA3					x	x	x	x	x								
FCS_CKM.1/CAM		x					x	x	x								
FCS_COP.1/CAM		x					x	x	x								
Class FIA																	
FIA_API.1/CA3					x	x	x	x	x								x
FIA_UAU.5/PACE_EAC2PP					x	x	x	x	x								x
FIA_UAU.6/CA3					x	x	x	x	x								
FIA_UID.1/PACE_EAC1PP		x	x				x	x	x		x						
FIA_UAU.5/PACE_EAC1PP		x	x				x	x	x		x						
FIA_API.1/PACE_CAM		x					x	x	x								
FIA_UAU.1/SSCDPP														x	x		
Class FDP																	
FDP_ACF.1/TRM			x	x		x	x		x		x		x				
Class FMT																	
FMT_SMR.1	x			x		x	x	x	x	x	x		x				
FMT_LIM.1/Loader																x	
FMT_LIM.2/Loader																x	
Class FTP																	
FTP_ITC.1/CA3					x		x	x	x								
Class FPT																	
FPT_EMS.1/EAC1PP											x	x	x				
FPT_EMS.1/EAC2PP				x								x	x				
FPT_EMS.1/SSCDPP													x				

Table 4: Coverage of Security Objectives for the TOE by SFRs

According to [CC1], tracing between SFRs and security objectives must ensure that 1) each SFR traces back to at least one security objective, and 2) that each security objective for the TOE has at least one SFR tracing to it. This is illustrated for

1. SFRs that have been newly added or refined within this PP by checking the *rows* of Table 4, and for SFRs that are merely iterated or simply included due to claims of other protection profiles by looking up the rationale of that PP
2. for newly introduced security objectives in this PP by checking the non-cursive *columns* of Table 4, and for the other security objectives by looking up the rationale of that PP.

In other words, in Table 4, we list only:

– SFRs that have been newly added or refined within this PP. Mere iterations or simple inclusions due to claims of other protection profiles are not listed however. For their coverage we refer to the respective claimed PP.

- Security objectives that are newly introduced in this PP, and their related SFRs.
- Security objectives for the TOE that are affected by the above newly added or refined SFRs.

Analogously, we limit our justification to the above SFRs and security objectives. For other security objectives, and for the justification of security objectives w.r.t. SFRs that are included or iterated from claimed protection profiles, we refer to the detailed rationales in [EAC1PP], [EAC2PP] and [SSCDPP].

OT.Chip_Auth_Proof_PACE_CAM is a newly introduced security objective that aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol, in particular in the context of an ePassport application. This is supported by **FCS_CKM.1/CAM** for cryptographic key-generation, and **FIA_API.1/PACE_CAM** and **FCS_COP.1/CAM** for the implementation itself, as well as **FIA_UID.1/PACE_EAC1PP** and **FIA_UAU.5/PACE_EAC1PP**, the latter supporting the PACE protocol.

OT.CA3 is a newly introduced security objective that aims to ensure the authenticity of the electronic document's chip while at the same time providing providing a very high level of protection against tracing. This is achieved by the Chip Authentication Version 3 (CA3) protocol. The security objective is supported by **FCS_CKM.1/CA3** for cryptographic key generation during CA3, and **FIA_API.1/CA3, FCS_COP.1/CA3** and **FIA_UAU.6/CA3** for the implementation of CA3 itself, **FTP_ITC.1/CA3** for secure communication with the TOE, as well as the refined SFRs **FIA_UAU.5/PACE_EAC2PP**, **FIA_UID.1/PACE_EAC1PP**, and **FIA_UAU.5/PACE_EAC1PP**.

The new **SFR FTP_ITC.1/CA3** provides an inter-trusted channel with the TOE using the CA3 protocol. The CA3 protocol is used to derive a shared secret, which itself provides encryption and integrity protection of the channel. Hence, the security objectives **OT.Data_Confidentiality** and **OT_Data_Integrity** are also supported by this SFR. The CA3 protocol itself is also used to authenticate the TOE to the communicating party. Therefore, **OT.Data_Authenticity** is supported by this SFR as well.

Aside the new SFRs mainly concerned with the above new security objectives, we discuss the remaining new and refined SFRs:

FIA_UAU.1/SSCDPP is refined here in a way that the TOE supports additionally EAC2 based access control w.r.t. SSCD-related user data. This does not affect the discussion of the rationale of [SSCDPP].
FDP_ACF.1/TRM unifies the access control SFPs of **FDP_ACF.1/TRM_EAC2PP** and **FDP_ACF.1/TRM_EAC1PP**. Both access control SFPs however are maintained w.r.t. sensitive EAC1-protected data and EAC2-protected data. Thus the discussion of the rationale of [EAC1PP] and [EAC2PP] remains unaffected.

FMT_SMR.1/EAC1PP and **FMT_SMR.1/EAC2PP** have been unified to **FMT_SMR.1** by adding additional roles. For all security objectives affected, FMT_SMR.1 supports related roles analogously as in the discussion of the rationales of [EAC1PP] and [EAC2PP].

The security objective **OT.Cap_Avail_Loader** is directly covered by the SFRs **FMT_LIM.1/Loader** and **FMT_LIM.2/Loader**, which limits the availability of the loader, as required by the objective.

FPT_EMS.1/EAC1PP and **FPT_EMS.1/EAC2PP** together define all protected data. Since all previous data are included, the discussion of the rationales of [EAC1PP] and [EAC2PP] is not affected.

The objective **OT.Non_Interfere** aims to ensure that no security related interferences between the implementations of the different access control mechanisms exist that allow unauthorized access of user or TSF-Data. This objective is fulfilled by enforcing the access control SFPs, in particular **FDP_ACF.1/TRM** in connection with **FDP_ACC.1/TRM_EAC1PP.** Related roles are supported by **FMT_SMR.1**. Interferences that are observable by emissions from the TOE are prevented due to **FPT_EMS.1/EAC1PP, FPT_EMS.1/EAC2PP, and FPT_EMS.1/SSCDPP**, where the set union of all defined data covers all relevant data.

6.3.2 Rationale for SFR's Dependencies

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

The dependency analysis has directly been made within the description of each SFR in Section 6.1 above. All dependencies being expected by [CC2] and by extended components definition in Chapter 5 are either fulfilled, or their non-fulfillment is justified.

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the predefined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

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

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

The selection of the component AVA_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry 'Attacker'). This decision represents a part of the conscious security policy for the electronic document required by the electronic document issuer and reflected by the current PP.

The set of assurance requirements being part of EAL4 fulfills all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance components: ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package. Below we list only those assurance requirements that are additional to EAL4.

ALC_DVS.2
Dependencies:
None

ATE_DPT.2
Dependencies:
ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
fulfilled by ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

AVA_VAN.5
Dependencies:
ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1
fulfilled by ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2

6.3.4 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) are internally consistent. The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

1510 The dependency analysis in Section 6.3.2 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately justified.

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

1515 The assurance package EAL4 is a predefined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in Section 6.3.3 shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements can only arise due to functional-assurance
1520 dependencies not being met. As shown in Section 6.3.2 and Section6.3.3,the chosen assurance components are adequate for the functionality of the TOE. Hence, there are no inconsistencies between the goals of these two groups of security requirements.

Glossary and Abbreviations

Glossary

Accurate Terminal Certificate
A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the electronic document's chip to produce terminal certificates with the correct certificate effective date, see [TR03110-3].

Card Access Number (CAN)
A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the electronic document), semi-static (e.g. printed on a label on the electronic document) or dynamic (randomly chosen by the electronic electronic document and displayed by it using e.g. ePaper, an OLED or similar technologies), cf. [TR03110-2].

Card Security Object (SO_C)
An RFC3369 CMS signed data structure signed by the Document Signer. It is stored in the electronic document (EF.CardSecurity, see [TR03110-3]) and carries the hash values of different data groups as defined. It also carries the Document Signer Certificate [TR03110-3].

Certificate Chain
Hierarchical sequence of Terminal Certificate (lowest level), DV Certificate and CVCA Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The CVCA Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).

Country Verifying Certification Authority (CVCA)
An organization enforcing the privacy policy of the electronic document issuer with respect to protection of sensitive user data that are stored in the electronic document. Practically, this policy is enforced when a terminal tries to get access to these sensitive user data. The CVCA represents the country specific root of the PKI for EAC1 terminals, EAC2 terminals resp. and creates DV certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA link-certificates, see [TR03110-3].

Current Date
The most recent certificate effective date contained in a valid CVCA link certificate, a DV certificate or an accurate terminal certificate known to the TOE, see [TR03110-3].

CV Certificate
Card verifiable certificate according to [TR03110-3].

CVCA Link Certificate
Certificate of the new public key of the CVCA signed with the old public key of the CVCA where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Security Object (SO_D)
A RFC3369 CMS signed data structure, signed by the Document Signer. Carries the hash values of the data groups. It is usually stored in an ICAO-conformant ePass application of an electronic document. It may carry the document signer certificate; see [TR03110-3]and [ICAO9303].

Document Signer
An organization enforcing the policy of the CSCA and signing the electronic document security object stored on the electronic document for passive authentication.
A document signer is authorized by the national CSCA to issue document signer certificate, cf. [TR03110-3] and [ICAO9303].
This role is usually delegated to the 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 resp., see [TR03110-3].

Extended Access Control 1
A set of security protocols and mechanisms to ensure genuineness of the electronic document and to allow a fine-grained access control to sensitive user data stored on an electronic document [TR03110-1].

Extended Access Control 2
A set of security protocols and mechanisms to ensure genuineness of the electronic document and to allow a fine-grained access control to sensitive user data stored on an electronic document [TR03110-2].

IC Dedicated Software
Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different entities. The usage of parts of the IC dedicated software might be restricted to certain life phases.

IC Embedded Software
Software embedded in an IC and not being designed by the IC developer. The IC embedded software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.

Electronic Document (electronic part only)
A smart card integrated into a plastic, optical readable cover. An electronic electronic document provides one or several application(s), such as an eID application, or an ePass application.

Initialization Data
Any data defined by the electronic document manufacturer and injected into the non-volatile memory by the integrated circuit manufacturer. These data are, for instance, used for traceability and for IC identification as IC_Card material (IC identification data).

Issuing State
The country issuing the electronic document; see [ICAO9303].

Machine Readable Zone (MRZ)
Fixed dimensional area located on the front of an ICAO-conformant electronic document. The MRZ contains mandatory and optional data for machine reading using optical character recognition; see [ICAO9303].
The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for PACE.

Meta-Data of a CV Certificate
Data within the certificate body as described in [TR03110-3]. The meta-data of a CV certificate comprise the following elements:

- Certificate Profile Identifier,
- Certificate Authority Reference,
- Certificate Holder Reference,
- Certificate Holder Authorization Template (CHAT),
- Certificate Effective Date,
- Certificate Expiration Date,
- Certificate Extensions (optional).

Passive Authentication
Security mechanism implementing (i) verification of the digital signature of the card (document) security object and (ii) comparing the hash values of the read data fields with the hash values contained in the card (document) security object. See [TR03110-3].

Password Authenticated Connection Establishment (PACE)
A communication establishment protocol defined in [TR03110-2] / [ICAO9303] resp.

PACE Password
A password needed for PACE authentication, e. g. CAN, MRZ, or a PIN.

Personal Identification Number (PIN)
A short secret password being only known to the electronic document holder. The PIN is a blocking password, see [TR03110-2].

Personalization
The process by which data related to the electronic document holder (biographic and biometric data, or key pair(s) for a potential signature application) are stored in and unambiguously, inseparably associated with the electronic document.

PIN Unblock Key (PUK)
A long secret password being only known to the electronic document holder. The PUK is a non-blocking password, see [TR03110-2].

Pre-personalization Data
Any data that is injected into the non-volatile memory of the TOE by the manufacturer for traceability of the non-personalized electronic document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.

Restricted Identification
Restricted Identification is a mechanism consisting of a security protocol for pseudo anonymization. This is achieved by providing a temporary electronic document identifier specific for a terminal sector and supporting related revocation features (see [TR03110-2]).

Secure Messaging
Secure messaging using encryption and message authentication code according to [ISO7816-4].

Abbreviations

CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CHAT	Certificate Holder Authorization Template
EAC	Extended Access Control
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number

	PP	Protection Profile
	PUK	PIN Unblock Key
	RF	Radio Frequency
1655	SAR	Security assurance requirements
	SFR	Security functional requirement
	TA	Terminal Authentication
	TOE	Target of Evaluation
	TSF	TOE security functionality
1660	TSP	TOE Security Policy (defined by the current document)
	VAD	Verification Authentication Data, cf. [SSCDPP]
	SVD	Signature Verification Data, cf. [SSCDPP]. The public key to verify a signature.

Reference Documentation

CC1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, 3.1, Revision 4
CC2	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, 3.1, Revision 4
CC3	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, 3.1, Revision 4
CC4	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004 , 3.1, Revision 4
EAC1PP	BSI: Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 v1.3.2 (5. December 2012)
EAC2PP	BSI: Common Criteria Protection Profile - ID-Card implementing Extended Access Control 2 as defined in BSI TR-03110, BSI-CC-PP-0086-2015 v1.01 (May 20th, 2015)
ICAO9303	ICAO: ICAO Doc 9303 - Machine Readable Travel Documents, 7th edition, 2015
ICPP	Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics: Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, v1.0 (13.01.2014)
ISO14443	ISO/IEC 14443 Identification cards — Contactless integrated circuit cards,
ISO7816-4	ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange,
PACEPP	BSI: Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011
SSCDPP	CEN: Standard InspectionCEN: Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-2:2012, v2.01, 01-2012, BSI-CC-PP-0059-2009-MA-01
TR03110-1	BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.10 (20. March 2012)
TR03110-2	BSI: TR-03110-2 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) v2.10 (20. March 2012)
TR03110-2-v2.20	BSI: TR-03110-2 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 2 – Protocols for electronic IDentification, Authentication and trust Services(eIDAS), v2.20 (3. February 2015)
TR03110-3	BSI: TR-03110-3 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 3 - Common Specifications v2.10 (20. March 2012)